intelbras

Manual do usuário

SG 2404 MR

intelbras

Switch Gerenciável 24 Portas Gigabit Ethernet com 4 Portas Mini-GBIC Compartilhadas

SG 2404 MR

Parabéns, você acaba de adquirir um produto com a qualidade e segurança Intelbras.

O switch SG 2404 MR possui 24 portas Gigabit Ethernet 10/100/1000 Mbps com 4 portas Mini-GBIC compartilhadas, proporcionando altas taxas de transferência de dados, permite a integração de computadores, impressoras, dispositivos VoIP como ATA e telefone IP, além de compartilhamento de internet para os demais dispositivos conectados a ele (dependendo do tipo de acesso e equipamento de banda larga disponível). Este switch integra múltiplas funções com excelente desempenho e fácil configuração.

Índice

1. Sobre o manual 5

1.1. Público destinado para o manual .5
1.2. Convenções .5
1.3. Estrutura do manual. .5

2. Introdução 7

2.1. Especificações técnicas. .7
2.2. Visão geral do switch .9
2.3. Principais funções .9
2.4. Descrição do produto .9

3. Acesso à interface de gerenciamento 11

3.1. Login .11
3.2. Configuração .12

4. System 12

4.1. System info .12
4.2. User manage .17
4.3. System tools .18
4.4. Access security .20

5. Switching 27

5.1. Port .27
5.2. LAG. .32
5.3. Traffic monitor .35
5.4. MAC address .37

6. VLAN 42

6.1. 802.1Q VLAN .43
6.2. MAC VLAN .47
6.3. Protocol VLAN .48
6.4. Exemplos de aplicação para 802.1Q VLAN .52
6.5. Exemplos de aplicação para MAC VLAN .53
6.6. Exemplos de aplicação de VLAN por Protocolo .54
6.7. GVRP. .55

7. Spanning tree 58

7.1. STP config .61
7.2. Port config. .63
7.3. MSTP instance .65
7.4. STP security .68
7.5. Exemplos de aplicações para STP .70

8. Multicast 73

8.1. IGMP snooping .75
8.2. Multicast IP .81
8.3. Multicast filter .83
8.4. Packet statistics .86

9. QoS 87
9.1. DiffServ 89
9.2. Bandwidth control 93
9.3. Voice VLAN 95
10. ACL 99
10.1. Time-Range 99
10.2. ACL config 101
10.3. Policy config 105
10.4. Policy binding 107
10.5. Exemplos de aplicação para ACL 109
11. Network security 110
11.1. IP-MAC binding 110
11.2. ARP inspection 117
11.3. DoS defend 123
11.4. 802.1X 125
12. SNMP 131
12.1. SNMP config 132
12.2. Notification 138
12.3. RMON 139
13. Cluster 142
13.1. NDP 143
13.2. NTDP 146
13.3. Cluster 149
13.4. Exemplo de aplicação da função Cluster 151
14. Maintenance 152
14.1. System monitor 152
14.2. Log 153
14.3. Device diagnose 156
14.4. Network diagnose 158
15. Restaurando para o padrão de fábrica 159
Termo de garantia 161

1. Sobre o manual

Este manual contém informações para instalação e gerenciamento do switch SG 2404 MR. Por favor, leia este manual com atenção antes de operar o produto.

1.1. Público destinado para o manual

Este manual é destinado a gerentes de redes familiarizados com conceitos de TI.

1.2. Convenções

Neste manual as seguintes convenções serão usadas:

» *System → System Info → System Sumary*: significa que a página *System Sumary* está dentro do submenu *System Info*, que está localizada dentro do menu System Menu.

» *Itálico* indica um botão, um ícone na barra de ferramentas, menu ou um item de menu.

Avisos	**Descrição**
Obs.:	Informações importantes para auxiliar o switch a ter um melhor desempenho e evitar danos ao produto.

1.3. Estrutura do manual

Capítulo	**Introdução**
1 - Sobre o manual	Introdução de como o manual está estruturado.
2 - Introdução	Introdução das funções, aplicação e aparência do SG 2404 MR.
3. Acesso à Interface de Gerenciamento	Introdução para logar na interface de gerenciamento web do produto.
4 - System	Este módulo é utilizado para configurações do sistema e propriedades do switch. A seguir as principais informações: - System Info: configurar a descrição, tempo do sistema e parâmetros de redes do switch. - User Manage: configuração de usuários e senhas, além de configurar o nível de acesso para cada usuário. - System Tools: gerenciamento dos arquivos de configuração do switch. - Access Security: fornece diferentes medidas de segurança para acessar o gerenciamento web do switch.
5 - Switching	Este módulo é utilizado para configurações básicas do switch. A seguir as principais informações: - Port - Configuração básica de portas. - LAG - Configuração de Agregação de Link (Link Aggregation Group - LAG). LAG permite a utilização de múltiplas portas para permitir o aumento da velocidade do link. - Traffic Monitor - monitor de tráfego em cada porta. - MAC Address - configuração da tabela de endereços MAC do switch.
6 - VLAN	Este módulo é utilizado para configurar VLANs. A seguir as principais informações: - 802.1Q VLAN: configuração de VLANs baseada em portas. - MAC VLAN: configuração de VLANs baseado em MAC, sem alterar a configuração 802.1Q VLAN. - Protocol VLAN: configuração de VLANs baseada em protocolos. - GVRP: o switch adiciona e remove VLANs automaticamente e transmite as novas informações de registros de VLANs para outros switches, sem a necessidade de configurar cada VLAN individualmente.
7 - Spanning Tree	Este módulo é utilizado para configurar a função de spanning tree no switch. A seguir as principais informações: - STP Config: configura e visualiza as configurações globais da função spanning tree. - Port Config: configura parâmetros da função STP para cada porta. - MSTP Instance: configura a instância MSTP. - STP Security: configura a proteção contra ataques maliciosos à função STP.
8 - Multicast	Este módulo é utilizado para configurar a função Multicast do switch. A seguir as principais informações: - IGMP Snooping: configuração global dos parâmetros IGMP Snooping, propriedade da porta, VLAN e Multicast VLAN. - Multicast IP: configuração da tabela de IP Multicast. - Multicast Filter: configuração dos recursos de filtros de endereços Multicast. - Packet Statistics: visualiza o tráfego de mensagens IGMP em cada porta do switch.
9 - QoS	Este módulo é utilizado para configuração de QoS, provendo qualidade e priorizando serviços desejados. A seguir as principais informações: - DiffServ: configuração de prioridade por porta, 802.1P e DSCP, além de configuração do algoritmo de escalonamento. - Bandwidth Control: controle de Banda por porta e configuração do Storm Control. - Voice VLAN: configuração de Voice VLAN para garantir a prioridade e qualidade na transmissão do fluxo de voz dentro de uma VLAN específica.

10 - ACL	Este módulo é utilizado para filtrar pacotes através de regras e políticas predeterminadas, a fim de controlar o acesso de usuários e pacotes ilegais à rede. A seguir as principais informações: - Time-Range: configuração do tempo efetivo para a aplicação das regras de ACL. - ACL Config: criação e configuração de regras para as ACLs. - Policy Config: configuração de políticas de ACL. - Policy Binding: vincula a política de ACL para uma porta ou VLAN específica.
11 - Network Security	Este módulo é utilizado para configurar medidas de proteção para a segurança da rede. A seguir as principais informações: - IP-MAC Binding: permite vincular o endereço IP, endereço MAC, VLAN ID e o número da porta do switch que o host está conectado, permitindo o acesso à rede. - ARP Inspection: configurar a inspeção ARP para prevenir ataques ARP na rede. - DoS Defend: configuração de proteção a ataques de negação de serviço (Denial of Service). - 802.1X: configuração de controle de acesso à rede baseado em portas, provendo um mecanismo de autenticação aumentando o segurança da rede.
12 - SNMP	Este módulo é utilizado para configurar a função SNMP, provendo um monitoramento e gerenciamento do switch na rede. A seguir as principais informações: - SNMP Config: define as configurações globais da função SNMP. - Notification: configuração das notificações (Trap e Inform) para gerenciamento e monitoramento dos eventos. - RMON: configuração da função RMON para monitorar a rede de forma mais eficiente.
13 - CLUSTER	Este módulo é utilizado para configurar a função de cluster, utilizando os protocolos NDP e NTDP para descoberta de vizinhos e manutenção da Topologia que envolve os dispositivos do Cluster. A seguir as principais informações: - NDP: protocolo utilizado para obter informações dos dispositivos vizinhos diretamente conectados. - NTDP: protocolo utilizado pelo switch principal para coletar as informações da topologia da rede. - Cluster: permite configurar o switch para pertencer a uma topologia com cluster ativo.
14 - Maintenance	Este módulo é utilizado para monitorar e gerenciar o switch. A seguir as principais informações: - System Monitor: monitoramento da memória e CPU do Switch. - Log: permite classificar, visualizar e gerenciar informações do sistema de forma eficaz. - Device Diagnose: testa o status da conexão do cabo conectado ao switch, testa se a porta do switch e o dispositivo conectado estão disponíveis. - Network Diagnose: testa se o endereço IP de destino está ao alcance do switch, bem como a quantidade de saltos necessários até alcançá-lo.
15 - Restaurando para o padrão de fábrica	Como restaurar o switch ao padrão de fábrica.

2. Introdução

2.1. Especificações técnicas

Chipset		Broadcom BCM53314S + BCM54685*2
Dimensões (CxAxL)		440x220x44 mm - Padrão EIA 19" com 1 U de altura
Material		Aço
LED	Power	Verde
	System	Verde
	Link/Act	Verde
	1000 Mbps	Verde e amarelo
Portas	10/100/1000M (RJ45)	24
	Mini GBIC (SFP)	4 (compartilhadas com as portas 21,22,23 e 24)
	Console (RJ45)	1
Cabeamento suportado	10BASE-T	Cabo UTP/STP categoria 3, 4, 5 (máximo 100m)
		EIA/TIA-568 100Ω STP (máximo 100m)
	100BASE-TX	Cabo UTP/STP categoria 5, 5e (máximo 100m)
		EIA/TIA-568 100Ω STP (máximo 100m)
	1000BASE-T	Cabo UTP/STP categoria 5e, 6 (máximo 100m)
		EIA/TIA-568 100Ω STP (máximo 100m)
	1000BASE-X	Fibras Monomodo e Multimodo
Padrões e protocolos	Padrão IEEE	IEEE802.3, 802.3u, 802.3ab, 802.3z, 802.3x, 802.1p, 802.1Q , 802.1x, 802.1d, 802.1w, 802.1s, 802.1v, 802.3ac
	Padrão IETF	RFC1541, RFC1112, RFC2236, RFC2618, RFC1757, RFC1157, RFC2571, RFC2030
	Outros padrões e protocolos	CSMA/CD, TCP/IP, SNMPv1/v2c/v3, HTTP, HTTPS, SSHv1/v2
Características básicas	Método de comutação	Armazena e envia (Store-and-Forward)
	Capacidade comutação	48 G
	Tabela endereço MAC	8 K
	Jumbo Frame	10240 Bytes
	Taxa de encaminhamento de pacote	35.7 Mpps
	VLAN	4 K VLANs ativas
		4 K VID
	Agregação de link (LAG)	8 grupos
		8 portas por grupos
	Multicast	256 grupos
	QOS (Quality of Service)	4 Filas de prioridade
	IP-MAC-PORT-VLAN Binding	200 entradas
	Número de ACL	200
Características	Configuração de portas	Auto negociação
		Controle de fluxo
		Espelhamento de portas
		Estatísticas de tráfego
	Agregação de link	Agregação de link Manual
		Agregação de link Dinâmica (LACP)
		Algoritmo baseado em endereço MAC de origem e destino
		Algoritmo baseado em endereço IP de origem e destino
	Tabela MAC	Filtro de endereço MAC
		Endereço MAC Estático
		Endereço MAC Dinâmico

Características	VLAN	VLAN baseado em porta
		802.1Q Tag VLAN
		MAC VLAN
		VLAN por protocolo
		VLAN de gerenciamento
		Voice VLAN
		GARP/GVRP
	Spanning tree	802.1d spanning tree protocol (STP)
		802.1w rapid spanning tree protocol (RSTP)
		802.1s multiple spanning tree protocol (MSTP)
		Loop Guard
		Root Guard
		TC-BPDU Guard
		BPDU Guard
		BPDU Filter
	Gerenciamento Multicast	IGMP v1/v2/v3
		IGMP Snooping
		Fast Leave
		Multicast VLAN
		Static Multicast groups
		Multicast Filter
		IGMP statistics
	QOS	4 Filas de prioridade
		Algoritmos de escalonamento: SP, WRR, SP+WRR
		Prioridade por porta
		802.1p
		DSCP
		Storm Control (Broadcast, Multicast, Unknown unicast)
		Controle de banda por porta
	Segurança	Port Security
		ARP Guard
		DoS (Denial of Service)
		ACL nas camadas 2,3,4 (L2/L3/L4)
		Autenticação 802.1x (baseado por porta e endereço MAC)
		Autenticação RADIUS
		Guest VLAN
		SSLv2/SSLv3/TLSv1
		SSHv1/SSHv2
		Restrição à interface de gerenciamento baseado em endereço IP, MAC e Porta
	Gerenciamento	SNMP v1/v2c/v3
		RMON (4 grupos)
		Gerenciamento web (http/https)
		CLI (Telnet, Console, SSHv1/v2)
		Espelhamento de porta
		Atualização de firmware via TFTP/web
		Configuração backup/reload
	Manutenção	DHCP Cliente
		DHCP Snooping
		DHCP Option 82
		SNTP Cliente
		BOOTP Cliente
		Teste de Loopback
		Ping
		Tracert
		System Log
		CPU monitor

Alimentação	Entrada	100-240 VAC, 50/60 Hz
Ambiente	Temperatura de operação	0°C a 40°C
	Temperatura de armazenamento	-40°C a 70°C
	Umidade de operação	10% a 90% sem condensação
	Umidade de armazenamento	5% a 90% sem condensação
Emissão de segurança e outros		Anatel
		FCC Part 15 B Class A
		CE: EN55022, EN61000-3-2, EN61000-3-3, EN55024, EN60950-1
		RoHS

2.2. Visão geral do switch

Projetado para grupos de trabalho e departamentos, o switch SG 2404 MR da Intelbras possui um alto desempenho e um conjunto completo de recursos de gerenciamento de camada 2. Ele fornece uma variedade de características com elevado nível de segurança. A capacidade de configuração inteligente fornece soluções flexíveis para uma escala variável de redes.

ACL, 802.1x e inspeção ARP fornecem uma robusta estratégia de segurança. QoS e IGMP Snooping/Filtering otimizam as aplicações de voz e vídeo. O LACP aumenta a largura de banda agregada, otimizando o transporte de dados, evitando gargalos na rede. SNMP, RMON, WEB/CLI/TELNET/SSH trazem uma grande variedade de políticas de gerenciamento. O SG 2404 MR traz múltiplas funções com excelente desempenho e facilidade de gerenciamento, o que corresponde a total necessidade dos usuários que exigem um grande desempenho da rede.

2.3. Principais funções

Resiliência e disponibilidade

- » Agregação de Link (LACP), aumenta a largura de banda agregada, otimizando o transporte de dados críticos.
- » IEEE802.1s Multiple Spanning Tree, oferece alta disponibilidade de link em ambientes com várias VLANs.
- » Snooping Multicast previne automaticamente a inundação de tráfego Multicast IP.
- » Root Guard, protege a bridge raiz de um ataque malicioso ou erros de configuração.

Protocolos da camada de enlaçe

- » GVRP, (GARP VLAN Registration Protocol) permite a criação automática de VLANs.
- » Suporte a 4K VLANs ativas e 4K VLAN ID.

Qualidade de serviço

- » Suporte QoS nas camadas 2/3 com até 4 filas de prioridade por porta.
- » Controle de banda por porta, limitando o tráfego de acordo com o valor determinado.

Segurança

- » Suporta vários padrões estabelecidos pela indústria e métodos de autenticação de usuário, como 802,1x, RADIUS.
- » Inspeção de ARP dinâmico, impedindo mensagens ARP não autorizado.
- » Lista de controle de acesso nas camadas 2/3/4 restringindo o acesso não confiável em um determinado recurso da rede.
- » Fornece criptografia de acesso SSHv1/v2, SSL 2.0/3.0 e TLS v1.

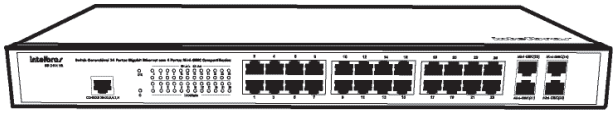
Gerenciamento

- » Suporta Telnet, CLI, SNMP v1/v2/v3, RMON e acesso web.

2.4. Descrição do produto

Painel frontal

O painel frontal do SG 2404 MR possui 24 portas Gigabit Ethernet 10/100/1000 Mbps e mais 4 portas Mini-GBIC compartilhadas, 1 porta console (RJ45) para gerenciamento via linha de comando, além de LEDs de monitoramento.



Painel frontal

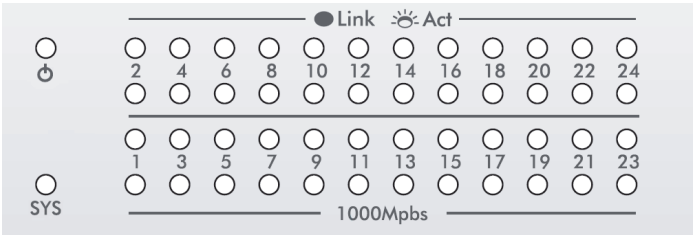
» **Portas 10/100/1000 Mbps:** 24 portas 10/100/1000 Mbps para conectar dispositivos com velocidade de 10 Mbps, 100 Mbps ou 1000 Mbps. Cada porta possui 2 LEDs correspondente.

» **Portas SFP:** 4 portas Mini-Gbic para conectar módulos SFP. As portas Mini-Gbic (21, 22, 23 e 24) são compartilhadas respectivamente com as portas RJ45 (21, 22, 23 e 24). As portas compartilhadas não podem ser utilizadas simultaneamente, caso contrário, somente as portas Mini-Gbic serão ativadas.

» **Porta Console:** 1 porta RJ45 para conectar com a porta serial de um computador para o gerenciamento e monitoramento do switch.

LEDs

No painel frontal são apresentados 50 LEDs de monitoramento, que seguem o comportamento abaixo:



LEDs

LED	STATUS	INDICAÇÃO
PWR	Aceso	Switch conectado a energia elétrica
	Piscando	Switch com problema na fonte de alimentação
	Apagado	Switch desligado ou com problema na fonte de alimentação
SYS	Aceso	Switch está funcionando de forma anormal
	Piscando	Switch funcionando normalmente
	Apagado	Switch está funcionando de forma anormal
Link/Act	Aceso	Conexão válida estabelecida, sem recepção/transmissão de dados
	Piscando	Conexão válida estabelecida, com transmissão/recepção de dados
	Apagado	Nenhuma conexão válida nesta porta, ou a porta está desativada
1000 Mbps	Aceso	Conexão válida estabelecida a 1000 Mbps estabelecida
	Apagado	A porta está conectada a um dispositivo 10/100 Mbps
		Nenhuma conexão válida nesta porta, ou a porta está desativada

Atenção: os slots Mini-GBIC (SFP) compartilham os mesmos LEDs indicadores com as portas 21, 22, 23 e 24.

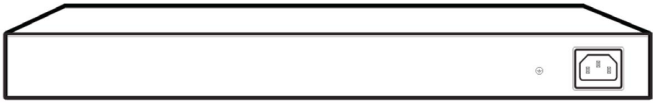
Obs.: *ao utilizar o slot Mini-GBIC (SFP) com um módulo de 100 Mbps ou 1000 Mbps, é necessário configurar a velocidade e o modo de transmissão correspondente ao módulo, acessando a interface de configuração no item Switching → Port → Port Config.*

Para módulos de 100 Mbps selecione 100 MFD, enquanto para os módulos de 1000 Mbps selecione 1000 MFD.

Por padrão, a velocidade e o modo de transmissão de uma porta SFP é 1000 MFD.

Painel posterior

O painel posterior possui um conector de alimentação de energia elétrica e um terminal de aterramento (representado pelo símbolo ⏚).



Painel posterior

» **Terminal de aterramento:** além do mecanismo de proteção a surto elétrico que o switch possui, você pode utilizar o terminal de aterramento a fim de garantir uma maior proteção. Para informações mais detalhadas, consulte o Guia de instalação.

» **Conector do cabo de energia:** para ligar o switch, conecte o cabo de energia (fornecido com o switch) no conector do switch e a outra ponta em uma tomada elétrica no padrão brasileiro de 3 pinos. Após energizá-lo, verifique se o LED PWR está aceso, indicando que o switch está conectado à rede elétrica e pronto para ser utilizado. Para compatibilidade com os padrões elétricos mundiais, este switch é projetado para trabalhar com uma fonte de alimentação automática com variação de tensão de 100 a 240 VAC, 50/60 Hz. Certifique-se que sua rede elétrica esteja dentro desta faixa.

3. Acesso à interface de gerenciamento

3.1. Login

1. Para acessar a interface de configuração, abra o navegador e na barra de endereços digite o endereço IP do switch: *http://192.168.0.1*, pressione a tecla *Enter*.

Endereço IP

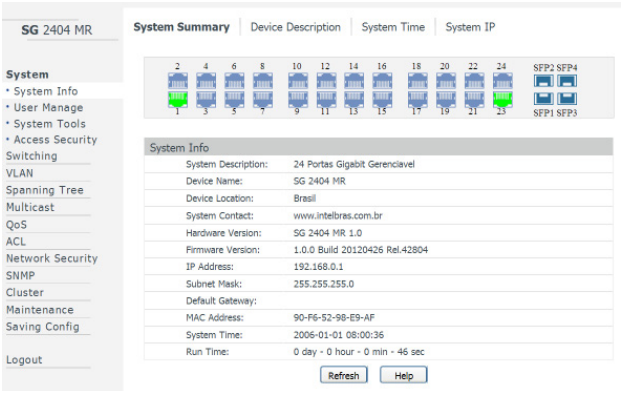
Obs.: *para efetuar o login no switch, o endereço IP do seu computador deve estar definido na mesma sub-rede utilizada pelo switch. O endereço IP 192.168.0.x (x sendo qualquer número de 2 à 254), e máscara de rede igual a 255.255.255.0.*

2. Após digitado o endereço IP do switch no navegador, será exibido a tela de login, conforme imagem a seguir. Digite *admin* para o nome de usuário e senha, ambos em letras minúsculas. Em seguida, clique no botão *Login* ou pressione a tecla *Enter*.

Tela de login

3.2. Configuração

Após realizado o Login, será possível configurar as funções do switch, clicando no menu de configuração localizado no lado esquerdo da tela, conforme imagem a seguir.



Tela de configuração

Obs.: *clicando em Apply as novas configurações ficarão ativas momentaneamente e serão perdidas ao reiniciar o switch. Para tornar as modificações permanentes no switch, por favor, clique em Saving Config.*

4. System

O menu System é utilizado para configuração do sistema e possui quatro sub-menus: *System Info, User Manage, System Tools* e *Access Security*.

4.1. System info

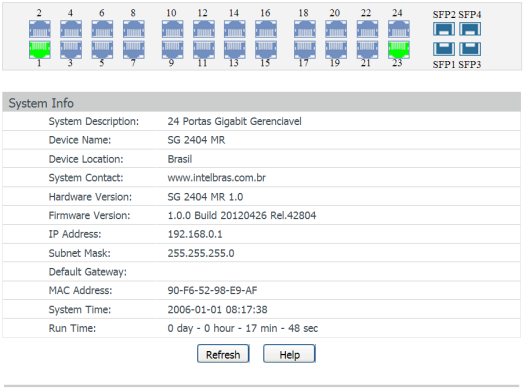
O sub-menu *System Info* é utilizado principalmente para as configurações básicas do switch. Este sub-menu possui os seguintes itens que podem ser configurados: *System Summary, Device Description, System Time* e *System IP*.

System summary

Nesta página é possível visualizar o status das conexões das portas e as informações do sistema.

O diagrama de portas, mostra o status das 24 portas 10/100/1000 Mbps RJ45 e das 4 portas SFP do switch.

Escolha o menu *System* → *System Info* → *System Summary* para carregar a seguinte página:



Sumário do sistema

» **Status das portas**

Indica que a porta 1000 Mbps não possui dispositivo conectado.

Indica que a porta 1000 Mbps possui um dispositivo 1000 Mbps conectado.

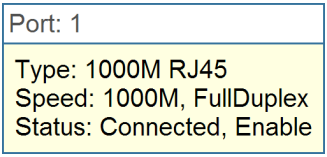
Indica que a porta 1000 Mbps possui um dispositivo 10 Mbps ou 100 Mbps conectado.

Indica que a porta SFP não possui dispositivo conectado.

Indicação de porta SFP possui um dispositivo 1000 Mbps conectado.

Indicação de porta SFP possui um dispositivo 100 Mbps conectado.

Ao passar o cursor do mouse por uma das portas, serão exibidas informações detalhadas referentes à porta desejada.



Detalhes da porta

» **Informações das portas**

Port: exibe o número da porta do switch.

Type: exibe o tipo de porta do switch.

Speed: exibe a taxa de transmissão máxima da porta.

Status: exibe o status de conexão da porta.

Clique na porta desejada para visualizar a largura de banda utilizada. A figura a seguir, exibe a largura de banda utilizada pela porta. O monitoramento é realizado a cada quatro segundos, facilitando a análise de detecção de problemas.

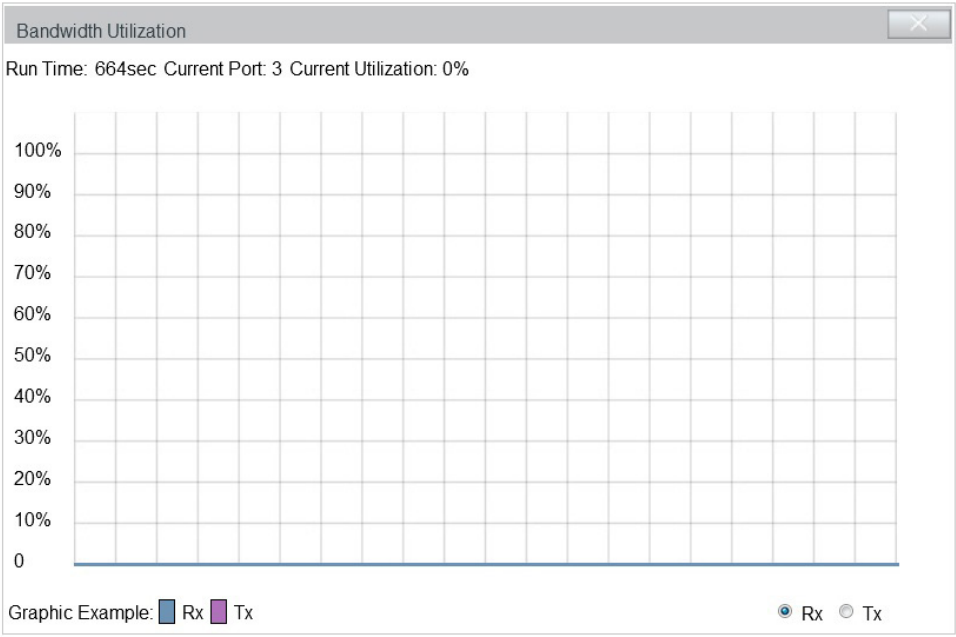


Gráfico de utilização da porta

» **Bandwidth utilization**

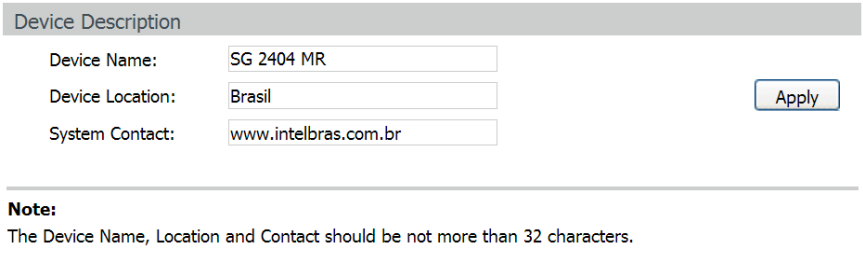
Rx: selecione *Rx* para exibir a banda utilizada na recepção de pacotes pela porta.

Tx: selecione *Tx* para exibir a banda utilizada na transmissão de pacotes pela porta.

Device Description

Nesta página você pode configurar a descrição do switch, incluindo o nome do dispositivo, localização do dispositivo e contato do sistema.

Escolha o menu *System* → *System Info* → *Device Description* para carregar a seguinte página.


Device Description
Device Name: SG 2404 MR
Device Location: Brasil
System Contact: www.intelbras.com.br
Apply
Note:
The Device Name, Location and Contact should be not more than 32 characters.

Descrição do switch

As seguintes opções são exibidas na tela:

» **Device description**

Device name: digite o nome de identificação do switch. Este campo permite no máximo 32 caracteres.

Device location: digite a localização do switch. Este campo permite no máximo 32 caracteres.

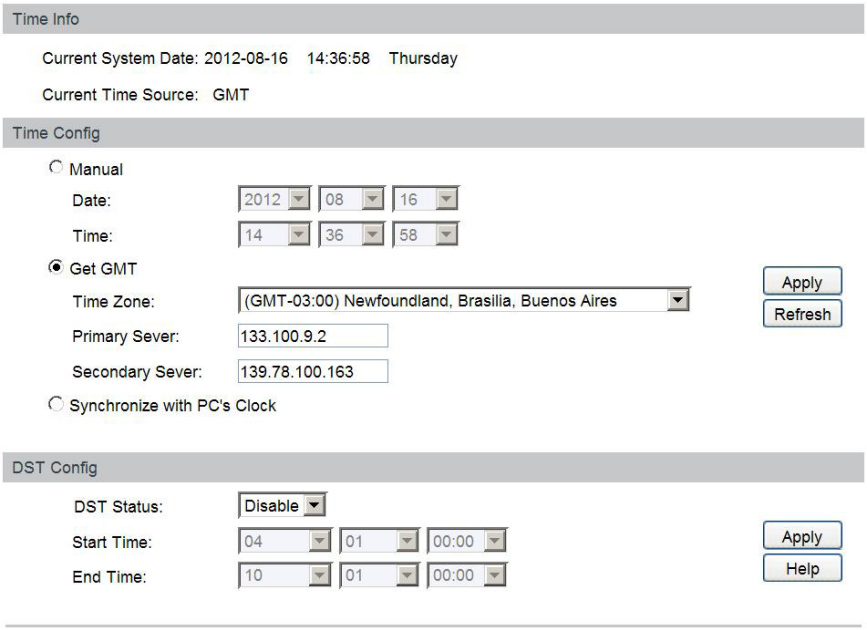
System contact: digite o contato do switch. Este campo permite no máximo 32 caracteres.

System time

Nesta página você pode configurar a data e hora do sistema que serão utilizadas por outras funções que necessitam deste tipo de informação, como por exemplo, ACL.

A configuração poderá ser realizada de forma automática, conectando-se a um servidor NTP, manualmente ou ainda sincronizando com a data e hora do computador.

Escolha o menu *System* → *System info* → *System Time* para carregar a seguinte página:



Data/Hora do sistema

As seguintes opções são exibidas na tela:

» **Time info**

Current system date: informa a data e hora atual do sistema.

Current time source: informa o modo de configuração da data e hora.

» **Time config**

Manual: quando esta opção estiver selecionada, você pode configurar a data e hora manualmente.

Get GMT: quando esta opção estiver selecionada, você pode configurar o fuso horário e o IP do servidor NTP. A mudança somente ocorrerá após o switch se conectar ao servidor NTP.

» **Time zone:** selecione o fuso horário desejado.

» **Primary/Secondary NTP server:** digite o endereço IP primário e secundário do servidor NTP.

» **Synchronize with PC's clock:** ao selecionar esta opção, a data e hora do switch serão sincronizadas com a data e hora do computador que está administrando o switch.

» **DST config**

DST status: habilita ou desabilita a função DST (Horário de verão).

Start time: selecione o dia e hora de início do horário de verão.

End time: selecione o dia e hora do término do horário de verão.

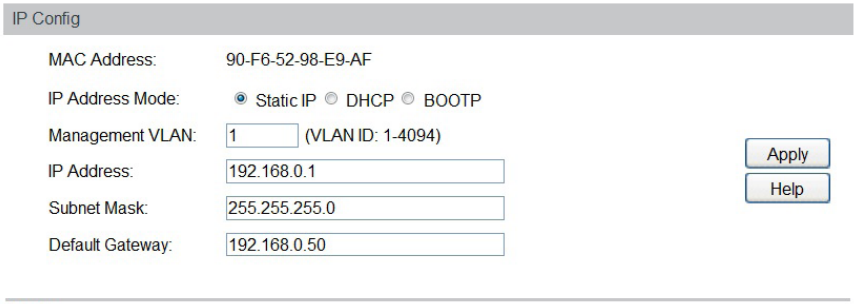
Obs.: » *A Data/Hora do sistema será reiniciada para o padrão quando o switch for reiniciado.*

» *Quando a opção Get GMT está selecionada e nenhum servidor NTP for encontrado, o switch receberá a data e hora do servidor de internet, se o switch estiver conectado a internet.*

System IP

Nesta página você pode configurar o endereço IP do swtich. Cada dispositivo na rede possui um endereço IP único. Você pode realizar o Login na interface web de gerenciamento do switch através de seu endereço IP. O switch suporta três modos para obtenção do endereço IP: Static IP, DHCP e BOOTP. Um endereço IP obtido utilizando um novo modo obtenção, substituirá o endereço IP corrente do switch.

Escolha o menu *System* → *System Info* → *System IP* para carregar a seguinte página:



Endereço IP

As seguintes opções são exibidas na tela:

» **IP config**

MAC address: exibe o endereço MAC do switch.

IP address mode: selecione o modo como o switch obterá o endereço IP.

» **Static IP:** quando esta opção for selecionada, você deverá digitar o endereço IP, máscara de rede e gateway padrão manualmente.

» **DHCP:** quando esta opção for selecionada, o switch receberá o endereço IP e parâmetros de rede através de um servidor DHCP.

» **BOOTP:** quando esta opção for selecionada, o switch receberá o endereço IP e parâmetros de rede através de um servidor BOOTP.

Management VLAN: digite a VLAN de gerenciamento do switch. Somente através da VLAN de Gerenciamento é possível obter acesso à interface de gerenciamento web do switch. Por padrão, a VLAN de Gerenciamento e todas as portas do switch estão configuradas na VLAN 1. No entanto, se outra VLAN for criada e definida para ser a VLAN de Gerenciamento, será necessário reconectar o computador em uma porta que pertence a VLAN de Gerenciamento para poder ter acesso à interface web do switch.

Subnet MASK: digite a máscara de sub-rede do switch quando estiver selecionado o modo Static IP.

Default gateway: digite o gateway padrão do switch quando estiver selecionado o modo Static IP.

Obs.: » *Alterando o endereço IP, para um IP localizado em uma sub-rede diferente, ocorrerá perda na comunicação com o switch. Para isso não acontecer, mantenha o endereço IP do switch dentro da mesma sub-rede da rede local.*

» *O switch possui somente um endereço IP. O endereço IP é configurável substituindo o endereço IP original.*

» *Se você configurar o switch para receber o endereço IP de um servidor DHCP, você poderá ver a configuração do endereçamento IP no servidor DHCP, se a opção DHCP for selecionada e não existir um servidor DHCP na rede, após alguns minutos o switch irá restaurar a configuração padrão.*

» *Se for escolhida a opção DHCP ou BOOTP, o switch irá receber parâmetros de rede dinâmicamente, então o endereço IP, máscara de rede e gateway padrão não poderão ser configurados.*

» *Por padrão, o endereço IP do switch é 192.168.0.1.*

4.2. User manage

O sub-menu User Manage é utilizado para realizar a configuração de usuários e senhas com níveis de acessos diferentes ao logar na página de gerenciamento web. Este sub-menu possui os seguintes itens: *User Table* e *User Config*.

User table

Nesta página você pode visualizar informações sobre os usuários correntes do switch.

Escolha o menu *System* → *User Manage* → *User Table* para carregar a seguinte página:

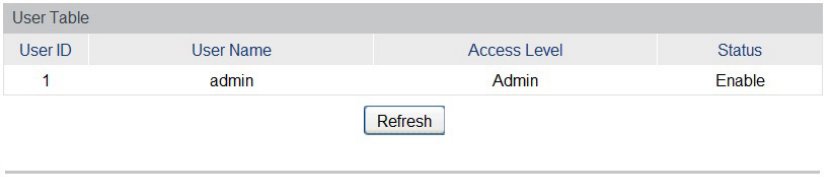
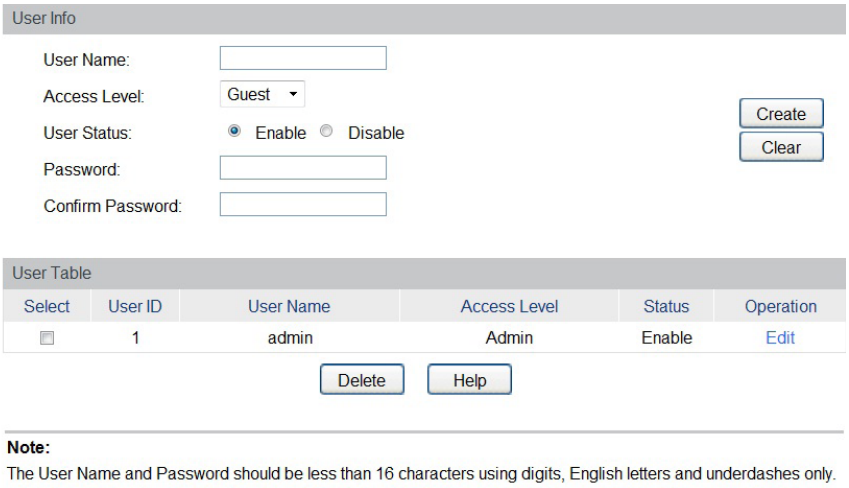


Tabela de usuários

User config

Nesta página você pode configurar os níveis de acesso que os usuários terão ao logar na página de gerenciamento web. O switch possui dois níveis de acesso: *Guest* e *Admin*. No nível de acesso guest, somente é possível visualizar as configurações do switch, já no nível de acesso admin, é possível realizar a configuração de qualquer função presente no switch.

Escolha o menu *System* → *User Manage* → *User Config* para carregar a seguinte página:



Configuração dos usuários

As seguintes opções são exibidas na tela:

» **User info**

User name: digite o nome de usuário que será criado.

Access level: selecione o nível de acesso do usuário ao realizar login.

» **admin:** admin pode editar, modificar e visualizar todas as configurações.

» **guest:** guest somente pode visualizar as configurações sem poder configurá-las.

User status: selecione *Enable/Disable* para habilitar ou desabilitar o usuário.

Password: digite a senha desejada para o usuário realizar o login.

Confirm password: repita a senha para confirmá-la.

» **User table**

Select: selecione o usuário desejado e clique no botão *Delete* para remover o usuário do sistema. O usuário corrente não poderá ser removido.

User ID, name, access level and status: exibe o ID, nome, nível de acesso e status do usuário.

Operation: clique no botão *Edit* para editar as informações do usuário correspondente. Após modificar as configurações, clique no botão *Modify* para validá-las. Não é possível modificar a configuração do usuário corrente.

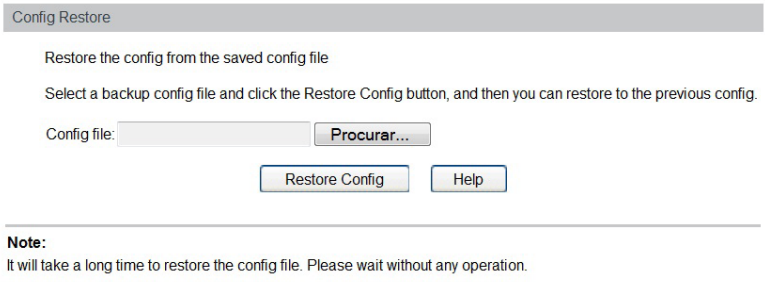
4.3. System tools

No sub-menu System Tools, é possível gerenciar os arquivos de configuração do switch, atualizar o firmware, reiniciar e restaurar ao padrão de fábrica. Este sub-menu possui cinco itens de configuração: *Config Restore, Config Backup, Firmware Upgrade, System Reboot* e *System Reset*.

Config restore

Nesta página você pode realizar o upload de um arquivo de configuração previamente salvo, restaurando o switch para uma configuração anterior.

Escolha o menu *System → System Tools → Config Restore* para carregar a seguinte página:


Config Restore
Restore the config from the saved config file
Select a backup config file and click the Restore Config button, and then you can restore to the previous config.
Config file:
Procurar...
Restore Config
Help
Note:
It will take a long time to restore the config file. Please wait without any operation.

Restauração das configurações

As seguintes opções são exibidas na tela:

» **Config restore:**

Restore config: selecione o arquivo de configuração previamente salvo em seu computador e clique no botão *Restore Config* para restaurar as configurações.

Obs.: *» A restauração das configurações levará alguns segundos. Por favor, espere sem realizar nenhuma outra operação.*

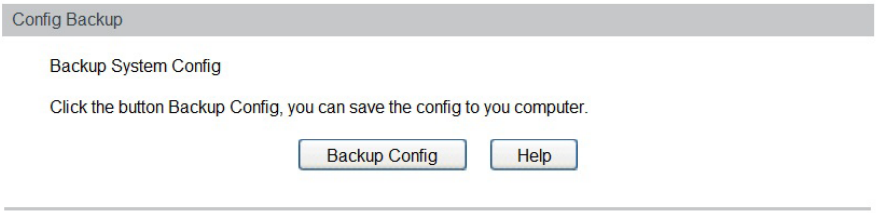
» Enquanto as configurações estiverem sendo restauradas, não desligue o switch da alimentação elétrica.

» Após serem restauradas, as configurações atuais serão perdidas, fazer o upload de um arquivo de backup errado pode fazer com que o switch perca o gerenciamento.

Config backup

Nesta página você poderá realizar o backup das configurações atuais do switch e salvá-los em um arquivo no seu computador, para uma restauração futura.

Escolha o menu *System* → *System Tools* → *Config Backup* para carregar a página.


Config Backup
Backup System Config
Click the button Backup Config, you can save the config to you computer.
Backup Config
Help
Note:
It will take a long time to backup the config file. Please wait without any operation.

Backup das configurações

As seguintes opções são exibidas na tela:

» **Config backup**

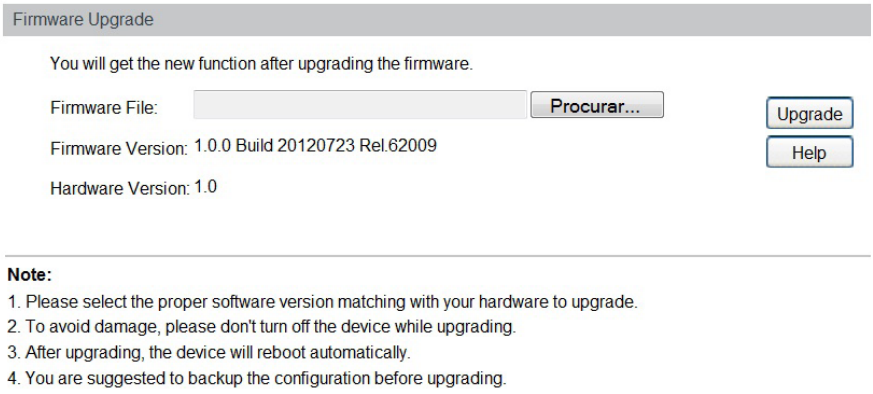
Backup config: clique no botão *Backup Config* para salvar as configurações atuais em um arquivo no seu computador. Essa sugestão pode ser adotada antes de realizar uma atualização.

Obs.: *o backup das configurações poderá levar alguns segundos.*

Firmware upgrade

O switch pode ser atualizado pela página de gerenciamento web. Para atualizar o sistema com a versão mais atualizada do firmware, faça o download através do site da Intelbras *www.intelbras.com.br.* É recomendável que seja feito um backup das configurações do switch antes do procedimento, pois a atualização do firmware pode causar a perda de todas as configurações existentes.

Escolha no menu *System* → *System Tools* → *Firmware Upgrade* para carregar a seguinte página:


Firmware Upgrade
You will get the new function after upgrading the firmware.
Firmware File:
Procurar...
Upgrade
Help
Firmware Version: 1.0.0 Build 20120723 Rel.62009
Hardware Version: 1.0
Note:
1. Please select the proper software version matching with your hardware to upgrade.
2. To avoid damage, please don't turn off the device while upgrading.
3. After upgrading, the device will reboot automatically.
4. You are suggested to backup the configuration before upgrading.

Atualização do firmware

Obs.: » *Não interrompa a atualização do switch.*

» *Selecione a versão de software apropriada para seu hardware.*

» *Após a atualização do firmware, o switch reiniciará automaticamente. Esta atualização poderá levar alguns minutos.*

» *É sugerido que você faça um backup das configurações antes de atualizar.*

System reboot

Nesta página é possível reiniciar o switch e retornar a página de login. Salve as configurações atuais antes de reiniciar o switch para evitar a perda das configurações realizadas que não foram salvas.

Escolha o menu *System* → *System Tools* → *System Reboot* para carregar a seguinte página.

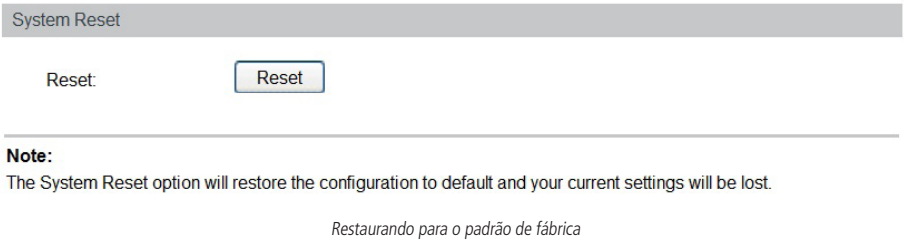
Reiniciando o Sistema

Obs.: *para evitar danos, por favor, não desligue o switch durante a reinicialização.*

System reset

Nesta página você pode restaurar o switch para a configuração padrão de fábrica. Todas as configurações serão perdidas após o switch reiniciar.

Escolha no menu *System* → *System Tools* → *System Reset* para carregar a página.


System Reset
Reset:
Reset
Note:
The System Reset option will restore the configuration to default and your current settings will be lost.

Restaurando para o padrão de fábrica

Obs.: *depois que o sistema reiniciar, todas as configurações serão restauradas para o padrão de fábrica.*

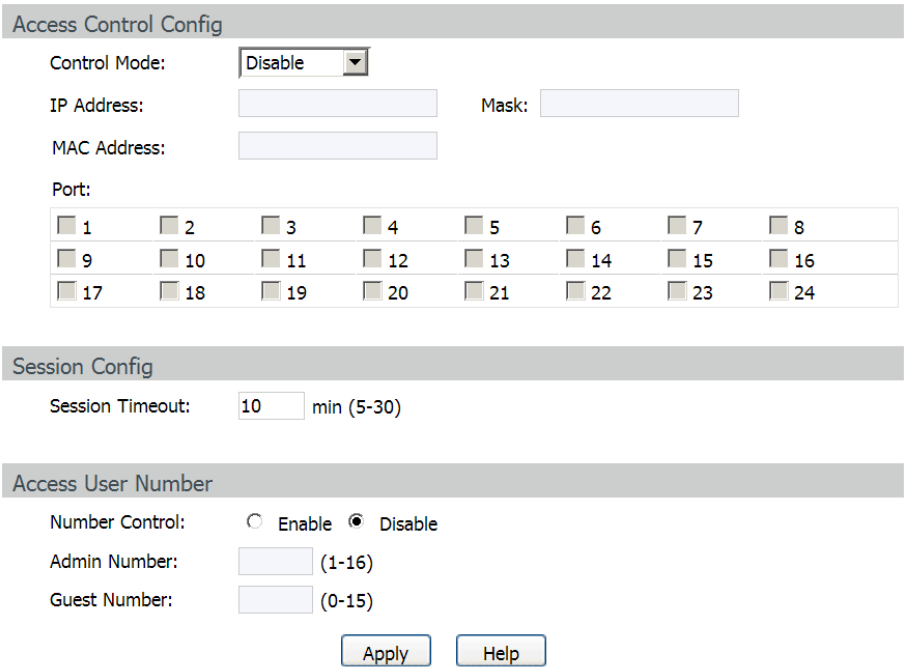
4.4. Access security

O sub-menu Access Security possui diferentes tipos de segurança para login remoto, aumentando o nível de segurança no gerenciamento do switch. Você pode realizar essas configurações através de três itens de configuração: *Access Control, SSL Config* e *SSH Config.*

Access control

Nesta página você pode controlar os usuários que poderão acessar a página de gerenciamento web. Para melhorar as configurações de segurança, utilize os níveis de acesso de usuário, explicado no capítulo 4.2. *User Manage.*

Escolha o menu *System* → *Access Security* → *Access Control* para carregar a seguinte página.



Controle de acesso

As seguintes informações são exibidas na tela:

» **Access control config**

Control mode: selecione o modo de controle de login para a página de gerenciamento web do switch.

» **IP-based:** selecione esta opção para especificar os endereços IPs dos computadores que poderão realizar login no switch.

» **MAC-based:** selecione esta opção para especificar os endereços MACs dos computadores que poderão realizar login no switch.

» **Port-based:** selecione esta opção para especificar em quais portas do switch os computadores deverão estar conectados para poder realizar login no switch.

IP Address&Mask: este campo somente estará disponível quando for selecionado o modo de controle IP-based. Somente o computador atual e os que estiverem dentro da faixa de endereços IPs poderão realizar login no switch.

MAC address: este campo somente estará disponível quando for selecionado o modo de controle MAC-based. Somente o computador atual e os que estiverem dentro da faixa de endereços MAC poderão realizar login no switch.

Port: este campo somente estará disponível quando for selecionado o modo de controle Port-based. Somente o computador atual e os que estiverem conectados as portas correspondentes poderão realizar login no switch.

» **Session config**

Session timeout: tempo em minutos de ociosidade do switch para desconectar o usuário. O tempo varia entre 5 e 30 minutos, o padrão é de 10 minutos.

» **Access user number**

Number control: selecione *Enable/Disable* para habilitar ou desabilitar a função de controle do número de usuário.

Admin number: digite o número máximo de usuários que poderão logar no switch com nível de acesso admin. Este número varia de 1 a 16 usuários simultaneamente.

Guest number: digite o número máximo de usuário que poderão logar no switch com nível de acesso guest. Este número varia de 0 a 15 usuários simultaneamente.

SSL config

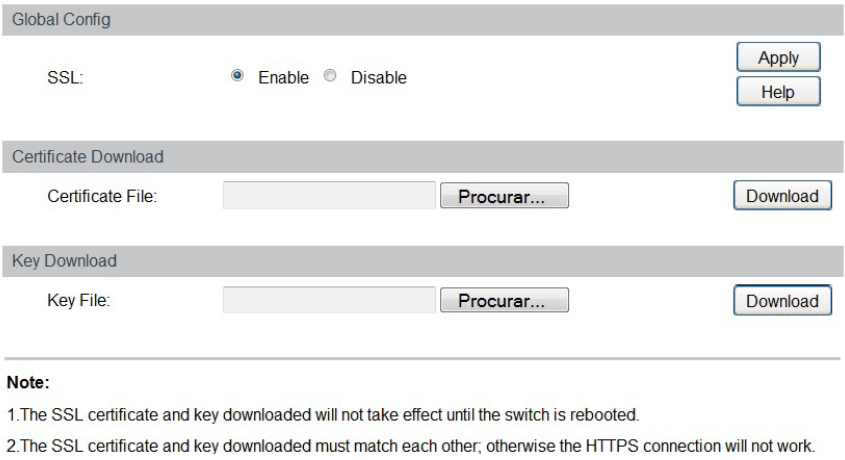
SSL (Secure Sockets Layer) é um protocolo de segurança, fornece uma conexão segura na camada de aplicação do modelo OSI (por exemplo, HTTP). SSL é utilizado para proteger a transmissão de dados entre o navegador da web e o servidor. É amplamente utilizado pelo comércio eletrônico e serviços bancários on-line. O SSL oferece os seguintes serviços:

1. Autenticar os usuários e os servidores com base em certificados, assegurando que os dados serão transmitidos para os servidores e usuários corretos.
2. Encriptação dos dados transmitidos, prevenindo uma interceptação ilegal dos pacotes.
3. Manter a integridade dos dados, garantindo que não serão alterados na transmissão.

Adotando a tecnologia de criptografia assimétrica, o SSL utiliza um par de chaves para criptografar e descriptografar as informações. Este par de chaves é referenciado como chave pública (contidas no certificado) e sua chave privada correspondente. Por padrão o switch possui um certificado autoassinado e uma chave privada correspondente. A opção *Certificate Download* e *Key Download* permite ao usuário substituir o par de chaves padrão do switch.

Após o SSL estar em funcionamento, você pode realizar login na interface web de gerenciamento do switch de forma segura, digitando *https://192.168.0.1*. Na primeira vez que você logar no switch com o SSL ativado, será exibida uma mensagem de erro de certificado, como por exemplo, "O Certificado de Segurança apresentado pelo site não foi emitido por uma Autoridade de Certificação confiável" ou "Erros de certificado". Por favor, adicione este certificado para certificados confiáveis ou clique em continuar no site.

Escolha no menu *System* → *Access Security* → *SSL Config* para carregar a seguinte página:



Configuração SSL

As seguintes opções são exibidas na tela:

» **Global config**

SSL: selecione *Enable/Disable* para habilitar ou desabilitar a função SSL do switch.

» **Certificate download**

Certificate File: selecione o certificado que deseja transferir para o switch, o certificado deverá ser codificado em BASE64.

» **Key download**

Key File: selecione a chave que deseja transferir para o switch. A chave deve ser codificada em BASE64.

Obs.: » *O certificado SSL e a chave devem ser correspondidas, caso contrário a conexão SSL não irá funcionar.*

» *O certificado SSL e a chave não terão efeitos até que o switch reinicie.*

» *Para estabelecer uma conexão segura durante a configuração do switch, digite na barra de endereço de seu navegador https://192.168.0.1.*

» *Uma conexão HTTPS pode demorar um pouco mais que uma conexão HTTP, isso porque em uma conexão HTTPS envolve autenticação, criptografia e descriptografia.*

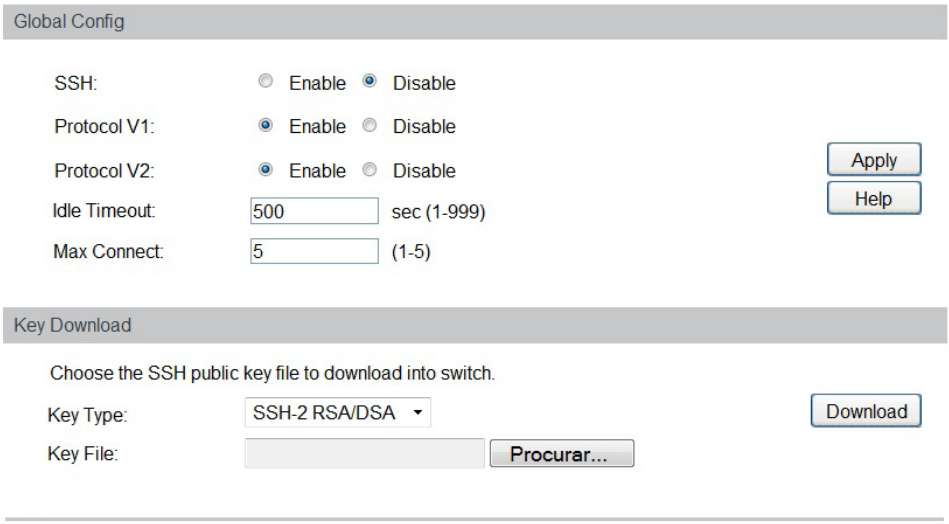
SSH config

Conforme estipulado pela IETF (Internet Engineering Task Force), o SSH (Secure Shell) é um protocolo de segurança estabelecido nas camadas de transporte e aplicação. A conexão criptografada do ssh é semelhante a uma conexão telnet, porém as conexões remotas como o telnet não são seguras, pois as senhas e os dados são transmitidos em forma de texto claro, isto é, não possui criptografia, sendo facilmente captadas e interpretadas por pessoas não autorizadas. O SSH provê informações de autenticação segura mesmo que você se autentique no switch através de um ambiente de rede inseguro. Ele criptografa todos os dados envolvidos na transmissão e evita que as informações sejam interceptadas.

O SSH é composto por um servidor e um cliente, possui duas versões, V1 e V2 que não são compatíveis entre si. Na comunicação entre o servidor e o cliente, o SSH pode negociar em qual versão irá operar e qual algoritmo de criptografia irá utilizar. Após realizar com sucesso a auto negociação o cliente envia a solicitação de autenticação ao servidor para o login. Somente após autenticado, a comunicação entre o cliente e o servidor será estabelecida.

O switch possui a função de servidor SSH, com isso, você pode instalar em seu computador um software SSH cliente para se conectar ao switch. A chave SSH pode ser salva no switch, se a chave for salva com êxito a autenticação de certificado dará preferência a essa chave.

Escolha no menu *System* → *Access Security* → *SSH Config* para carregar a seguinte página:



Configuração SSH

As seguintes informações são exibidas na tela:

» **Global config**

SSH: selecione *Enable/Disable* para habilitar ou desabilitar a função SSH.

Protocol V1: selecione *Enable/Disable* para habilitar ou desabilitar a versão v1 do SSH.

Protocol V2: selecione *Enable/Disable* para habilitar ou desabilitar a versão v2 do SSH.

Idle timeout: digite o tempo em segundos, em que o switch aguardará para desconectar a conexão SSH, caso esteja ociosa. Por padrão este tempo é de 500 segundos e pode variar de 1 a 999 segundos.

Max connect: digite o número máximo de conexões SSH que o switch suportará simultaneamente. O valor padrão é 5 e pode variar de 1 a 5.

» **Key download**

Key Type: selecione o tipo da chave que será utilizado pelo SSH. O switch suporta três tipos: SSH-1 RSA, SSH-2 RSA e SSH2-DSA.

Key File: selecione a chave correspondente ao tipo de chave utilizado para download.

Download: clique no botão *Download* para salvar a chave no switch.

Obs.: » *Por favor, tenha certeza que a chave SSH transferida possua tamanho entre 256 e 3072 bits.*

» *Após salvar a nova chave SSH, a chave original será substituída.*

» *Caso uma chave SSH seja salva erradamente, o acesso SSH será realizado através da senha de autenticação.*

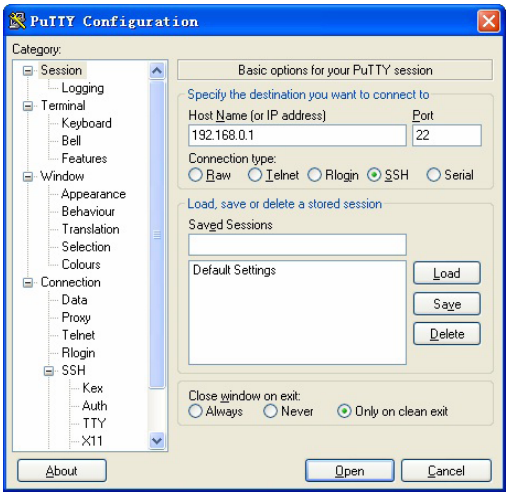
Primeiro exemplo de aplicação SSH

» **Requisitos de rede**

1. Faça Login no switch utilizando um software cliente SSH. A função *SSH* do switch deverá estar habilitada.
2. Recomendamos o uso do programa PuTTY como software cliente SSH.

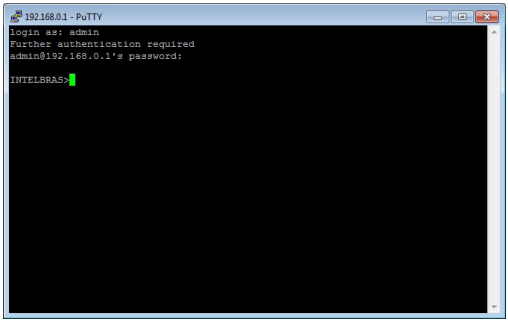
» **Procedimento de configuração**

1. Abra o programa PuTTY e digite o endereço IP do Switch no campo Host Name (or IP address), mantenha o valor padrão do campo Port como 22, selecione *Connection type* como SSH, conforme imagem a seguir.



Configuração do PuTTY

2. Clique no botão *Open* para fazer o login no switch. Será exibido um terminal de linha de comandos, digite o nome de usuário e senha do switch (usuário e senha padrão do switch é *admin*), após realizado o login, será possível gerenciar o switch através do terminal de linha de comando, conforme imagem a seguir.



Terminal de linha de comandos

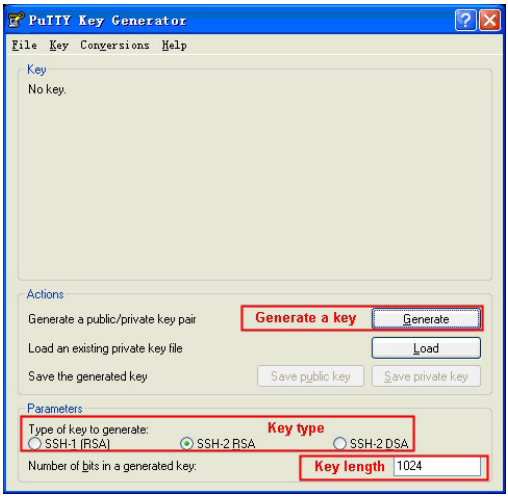
Segundo exemplo de aplicação SSH

» **Requisitos de rede**

1. Faça Login no switch utilizando um software cliente SSH, com chaves criptográficas geradas pelo usuário. A função SSH do switch deverá estar habilitada.
2. Recomendamos o uso do programa PuTTY como software cliente SSH, PuTTY Key Generator para a geração das novas chaves criptográficas e Pageant Key List para carregar a chave privada gerada. Todos estes programas estão disponíveis para download gratuitamente no site do fabricante do software PuTTY.

» **Procedimento de configuração**

1. Abra o programa PuTTY Key Generator e selecione o tipo e o comprimento da chave SSH e clique no botão *Generate*, conforme imagem a seguir:

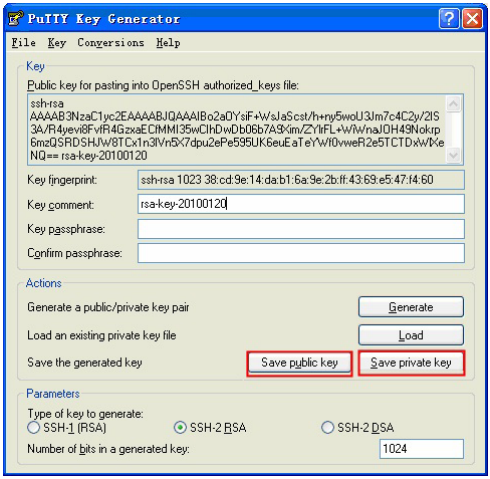


PuTTY Key Generator

Obs.: *» O comprimento da chave SSH deverá possuir tamanho entre 256 e 3072 bits.*

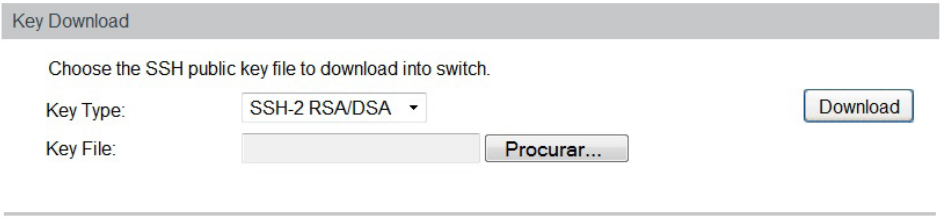
» Durante a geração da chave SSH, mova o cursor do mouse aleatoriamente para auxiliar no processo de geração da chave.

2. Após as chaves serem geradas com sucesso, por favor, salve-as em seu computador, utilizando os botões Save public Key e Save private Key, conforme imagem a seguir:



PuTTY Key Generator

3. Na página de gerenciamento web do switch, faça o download da chave pública gerada que está salva em seu computador para o switch, conforme imagem a seguir:

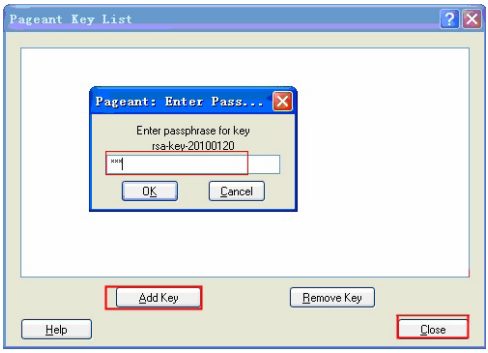

Key Download
Choose the SSH public key file to download into switch.
Key Type:
SSH-2 RSA/DSA
Download
Key File:
Procurar...
Note:
It will take a long time to download the key file. Please wait without any operation.

Download da chave SSH

Obs.: » *O tipo de chave configurada no switch deverá estar de acordo com o tipo de chave criada.*

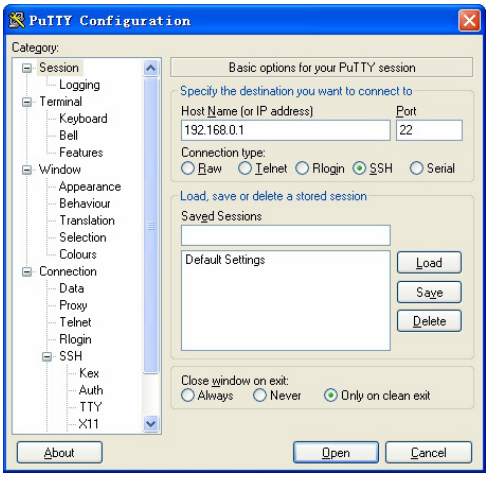
» *Não interrompa o download da chave SSH.*

4. Utilize o programa Pageant Key List para carregar a chave privada criada, que será utilizada pelo software cliente SSH, conforme imagem a seguir:



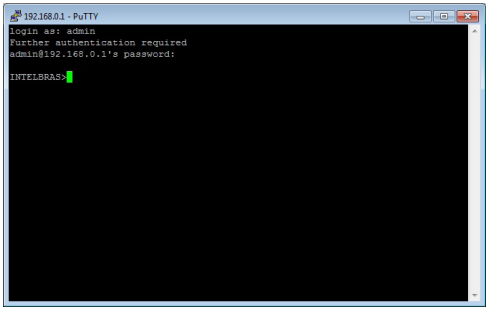
Carregando a chave privada

5. Após os procedimentos de criação e carregamento das chaves criptográficas, por favor acesse a interface do PuTTY e insira o endereço IP para login no switch, conforme imagem a seguir:



Conectando no switch via SSH

Após autenticação bem sucedida, digite o nome de usuário. Se você fizer login no switch sem precisar digitar a senha, significa que a chave foi salva com êxito, conforme imagem a seguir.



Autenticação bem sucedida

5. Switching

O menu Switching é utilizado para as configurações básicas do switch, incluindo quatro sub-menus: *Port, LAG, Traffic Monitor e MAC Address.*

5.1. Port

O sub-menu Port permite configurar recursos básicos utilizados pelas portas do switch, a configuração pode ser realizada nas seguintes páginas: *Port Config, Port Mirror, Port Security* e *Port Isolation.*

Port config

Nesta página são configurados os parâmetros básicos para as portas, quando a porta está desativada todos os pacotes serão descartados. Todos os parâmetros afetarão o modo de funcionamento das portas, por favor, defina os parâmetros das portas conforme sua necessidade.

Escolha o menu *Switching → Port → Port Config* para carregar a seguinte página:

Port Config

Port Select

Select	Port	Description	Status	Speed and Duplex	Flow Control	LAG
			Disable	10MHD	Disable	
	1		Enable	Auto	Disable	---
	2		Enable	Auto	Disable	---
	3		Enable	Auto	Disable	---
	4		Enable	Auto	Disable	---
	5		Enable	Auto	Disable	---
	6		Enable	Auto	Disable	---
	7		Enable	Auto	Disable	---
	8		Enable	Auto	Disable	---
	9		Enable	Auto	Disable	---
	10		Enable	Auto	Disable	---
	11		Enable	Auto	Disable	---
	12		Enable	Auto	Disable	---
	13		Enable	Auto	Disable	---
	14		Enable	Auto	Disable	---
	15		Enable	Auto	Disable	---

Apply Help

Note:
The Port Description should be not more than 16 characters.

Parâmetros das portas

As seguintes informações são exibidas na tela:

Port: digite o número da porta desejada dentro do campo correspondente e clique no botão *Select* para selecionar a porta.

Select: selecione a porta desejada para realizar a configuração. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Description: digite uma descrição para a porta.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a porta correspondente. Quando a porta estiver habilitada o switch poderá encaminhar os pacotes normalmente.

Speed and duplex: escolha a velocidade e o modo Duplex para porta. O dispositivo conectado ao switch deve estar na mesma velocidade e modo Duplex . Quando o modo *Auto* for selecionado o modo *Duplex* será determinado pela auto negociação. As portas SFP não suportam auto negociação.

Flow control: selecione *Enable/Disable* para habilitar ou desabilitar o controle de fluxo. Quando o Flow Control é ativado, o switch pode sincronizar a transmissão de dados, evitando a perda de pacotes causada por congestionamentos na rede.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Obs.: » *Não desabilite a porta usada para o gerenciamento do switch.*

» *As portas membros de um grupo LAG devem possuir os mesmos parâmetros de configuração de porta.*

» *Ao utilizar módulos SFP de 100 Mbps ou 1000 Mbps, é necessário configurar o parâmetro Speed and Duplex. Para módulos de 100 Mbps, selecione o modo 100MFD, para módulos Gigabit selecione 1000MFD. Por padrão o switch vem configurado com o modo 1000MFD.*

Port mirror

Nesta página é possível configurar o espelhamento de portas. Esta função permite o encaminhamento de cópias de pacotes de uma ou mais portas (mirrored port) para uma porta definida como porta espelho (mirroring port). Geralmente o espelhamento de portas é utilizado para realizar diagnósticos e análise de pacotes, a fim de monitorar e solucionar problemas na rede.

Escolha o menu *Switching* → *Port* → *Port Mirror* para carregar a seguinte página:

Mirror Group List

Group	Mirroring	Mode	Mirrored Port	Operation
1	0	Ingress	---	Edit
		Egress	---	
2	0	Ingress	---	Edit
		Egress	---	
3	0	Ingress	---	Edit
		Egress	---	
4	0	Ingress	---	Edit
		Egress	---	

Help

Espelhamento de portas

As seguintes opções são exibidas na tela:

» **Mirror group list**

Group: exibe o número do grupo das portas espelhadas.

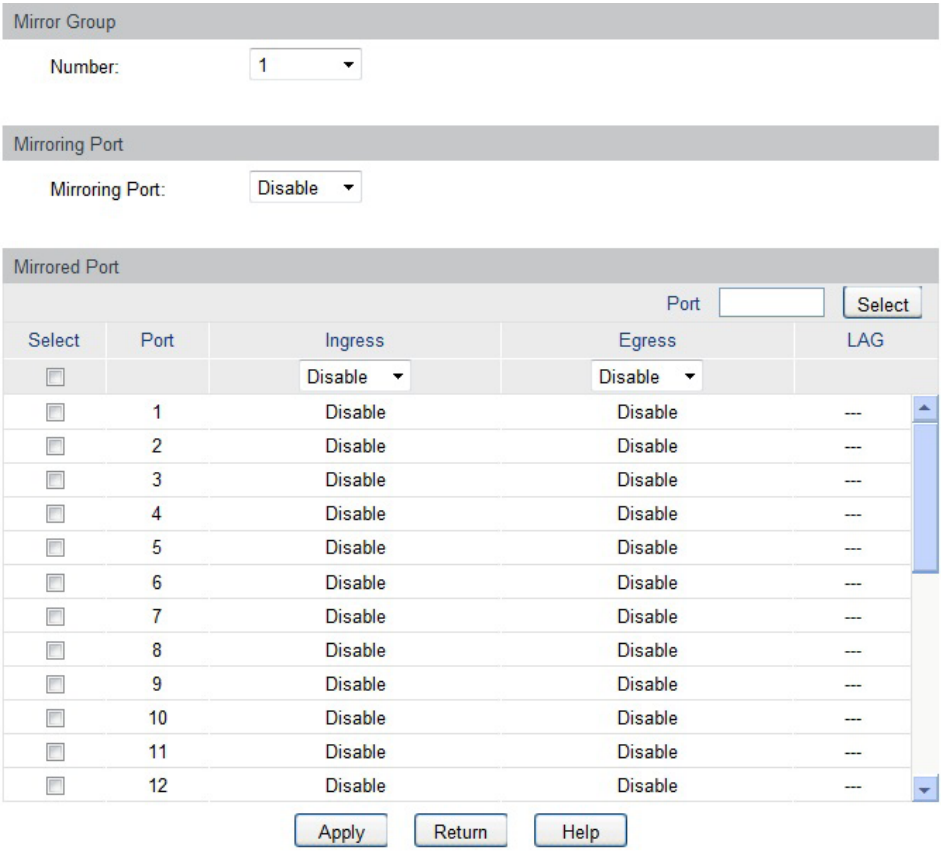
Mirroring: exibe o número da porta espelho (mirroring port).

Mode: exibe a direção dos pacotes espelhados, "Ingress" pacotes recebidos, "Egress" pacotes enviados.

Mirrored port: exibe as portas espelhadas (mirrored port).

Operation: clique em *Edit* para configurar o grupo de portas espelhadas.

Ao clicar em *Edit*, será exibido a seguinte página:



Configuração do espelhamento de portas

As seguintes informações são exibidas na tela:

» **Mirror group**

Number: selecione o grupo de portas espelhadas que deseja configurar.

» **Mirroring port**

Mirroring port: selecione a porta espelho (Mirroring Port)

» **Mirrored port**

Port: digite o número da porta espelhada (mirrored port) dentro do campo correspondente e clique no botão *Select* para selecionar a porta.

Select: selecione a porta espelhada (mirrored port). Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Ingress: selecione *Enable/Disable* para habilitar ou desabilitar o recurso de encaminhamento dos pacotes recebidos pela porta espelhada. Uma cópia desses pacotes será enviada para a porta espelho.

Egress: selecione *Enable/Disable* para habilitar ou desabilitar o recurso de encaminhamento dos pacotes enviados pela porta espelhada. Uma cópia desses pacotes será enviada para a porta espelho.

LAG: exibe o número do grupo LAG que a porta pertence. Uma porta membro de um grupo LAG não pode ser selecionada como porta espelhada ou porta espelho.

Obs.: » *Portas membros de um grupo LAG não podem ser selecionadas como porta espelhada ou porta espelho.*

» *Uma porta não pode ser simultaneamente porta espelhada e porta espelho.*

» *A função de espelhamento abrange varias VLANs.*

Port security

Quando um equipamento de rede é conectado a uma das portas do switch, este aprende o endereço MAC do dispositivo e cria uma associação entre o endereço MAC e o número da porta, criando uma entrada na tabela de encaminhamento (Tabela de endereços MAC). Esta tabela é a base para que o switch possa encaminhar os pacotes rapidamente, entre o endereço de origem e destino, diminuindo o tráfego em broadcast. Existem também recursos de filtragem de endereços MAC, permitindo que o switch filtre pacotes indesejados, proibindo seu encaminhamento e melhorando a segurança da rede.

Escolha no menu *Switching* → *Port* → *Port Security* para carregar a seguinte página:

Port Security

Select	Port	Max Learned MAC	Learned Num	Learn Mode	Status
☐				Dynamic	Disable
☐	1	64	0	Dynamic	Disable
☐	2	64	0	Dynamic	Disable
☐	3	64	0	Dynamic	Disable
☐	4	64	0	Dynamic	Disable
☐	5	64	0	Dynamic	Disable
☐	6	64	0	Dynamic	Disable
☐	7	64	0	Dynamic	Disable
☐	8	64	0	Dynamic	Disable
☐	9	64	0	Dynamic	Disable
☐	10	64	0	Dynamic	Disable
☐	11	64	0	Dynamic	Disable
☐	12	64	0	Dynamic	Disable

Apply Help

Note:
The maximum number of MAC addresses learned from individual port can be set to 64.

Port security

As seguintes informações são apresentadas na tela:

» **Port security**

Select: selecione a porta que será configurada o Port Security. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Max learnerd MAC: especifique o número máximo de endereços MAC que poderão ser aprendido pelo switch na porta desejada.

Learned num: exibe o número de endereços MAC que já fora aprendidos pela porta.

Leran Mode: selecione o modo de aprendizagem da porta.

» **Dynamic:** neste modo, o endereço MAC aprendido será excluído da tabela de endereços MAC automaticamente após terminar o tempo de envelhecimento (aging time).

» **Static:** neste modo, o endereço MAC deverá ser incluído ou removido manualmente, os endereços MAC estático não possuem tempo de envelhecimento (aging time).

» **Permanent:** neste modo, as entradas aprendidas somente poderão ser removidas manualmente, não participará do processo de envelhecimento (aging time) e também não serão apagadas ao reiniciar o switch.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a função *Port Security* para a porta desejada.

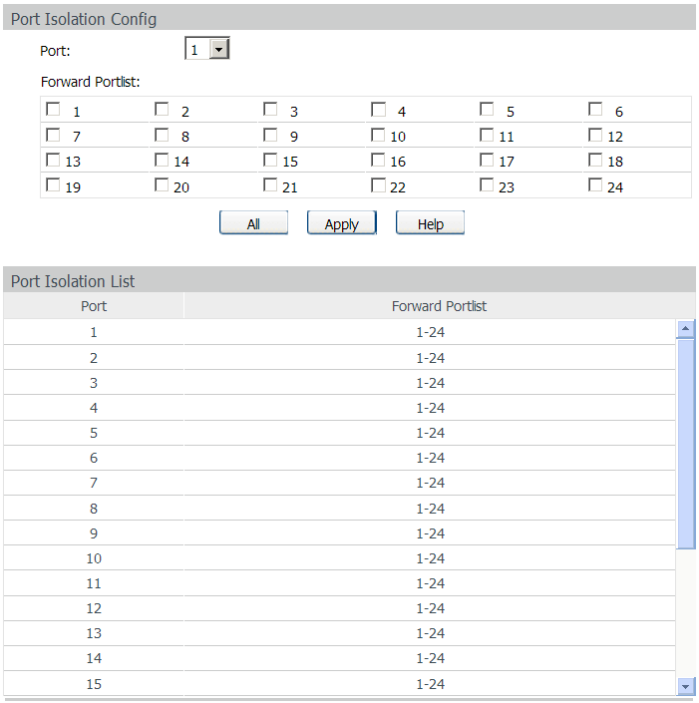
Obs.: » *A função Port Security será desabilitada para as portas membros de grupos LAG.*

» *A função Port Security será desabilitada quando a função 802.1X está ativada.*

Port isolation

Port Isolation fornece um método para restringir o fluxo do tráfego para melhorar a segurança da rede. Esta função basicamente permite que uma porta somente possa encaminhar pacotes para as portas que estão em sua lista de encaminhamento. Este método de segmentar o fluxo do tráfego é semelhante a utilização de VLANs, porém com mais restrições de configuração.

Escolha no menu *Switching* → *Port* → *Port Isolation* para carregar a seguinte página:



Port isolation

As seguintes informações são apresentadas na tela:

» **Port isolation config**

Port: selecione a porta que será configurada como Port Isolation.

Forward portlist: selecione as portas que poderão se comunicar com a porta configurada como Port Isolation. Nesta opção é possível selecionar mais de uma porta simultaneamente.

» **Port isolation list**

Port: exibe o número da porta do switch.

Forward portlist: exibe a lista de portas que poderão se comunicar com a porta configurada como Port Isolation.

5.2. LAG

LAG (Link Aggregation Group) é a função de agregação de links, permite a utilização de múltiplas portas para permitir o aumento da velocidade do link além dos limites nominais de uma única porta, introduz controle de falhas e redundância para a conexão a outro dispositivo que disponha do mesmo recurso. As portas pertencentes a um grupo LAG devem possuir os mesmos parâmetros de configuração, caso utilizadas com as seguintes funções: *STP, QoS, GVRP, VLAN, MAC Address Learning*. Seguem as explicações.

- » Portas que estiverem habilitadas as funções *GVRP, 802.1Q VLAN, Voice VLAN, STP, QoS, DHCP Snooping e Port Configuration (Speed e Duplex, Flow Control)* e que participam de um mesmo grupo LAG, deverão obrigatoriamente possuir as mesmas configurações.
- » Portas que estiverem habilitadas as funções P*ort Security, Port Mirror, MAC Address Filtering, Static MAC Address Binding* e *802.1X*, não poderão ser adicionadas a um grupo LAG.
- » Não é recomendado adicionar portas a um grupo LAG que estejam habilitadas com as funções *ARP inspection e DoS Defend*.

É recomendável configurar primeiramente os grupos LAG antes de configurar as demais funções.

Obs.: » *Como calcular a largura de banda em uma Agregação de Link: Suponhamos que um grupo LAG possua quatro portas com velocidade de 1000 Mbps Full Duplex, a largura de banda total do grupo LAG é de 8000 Mbps (2000 Mbps * 4) isto porque a largura de banda de cada porta é de 2000 Mbps, sendo 1000 Mbps de uplink e 1000 Mbps de downlink.*

» *O balanceamento de carga entre as portas pertencentes a um grupo LAG será de acordo com o algoritmo de balanceamento configurado. Se a conexão de uma porta estiver com perdas de pacotes, o tráfego será transmitido pelas portas que estejam normais. De modo a garantir a confiabilidade da conexão.*

A função de Agregação de Link é configurada nas páginas *LAG Table, Static LAG e LACP Config*.

LAG table

Nesta página você pode visualizar e configurar as informações atuais dos grupos LAG.

Escolha no menu *Switching → LAG → LAG Table* para carregar a seguinte página:

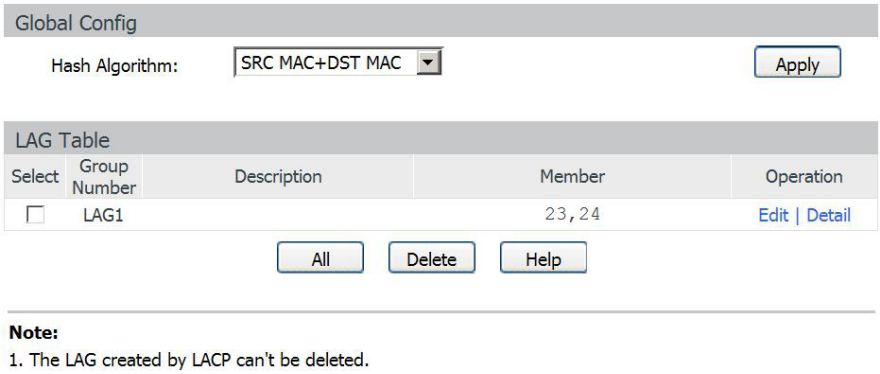


Tabela de agregação de link (LAG)

As seguintes informações são exibidas na tela:

- » **Global config**

  Hash algorithm: selecione o algoritmo de balanceamento de carga utilizado pelas portas de um grupo LAG.

  - » **SRC MAC + DST MAC:** este algoritmo utiliza o endereço de MAC de origem e de destino para realizar o balanceamento de carga.
  - » **SRC IP + IP DST:** este algoritmo utiliza o endereço IP de origem e de destino para realizar o balanceamento de carga.

- » **LAG table**

  Select: selecione o grupo LAG desejado. Nesta opção é possível selecionar mais de um grupo simultaneamente.

  Group number: exibe o número do grupo LAG.

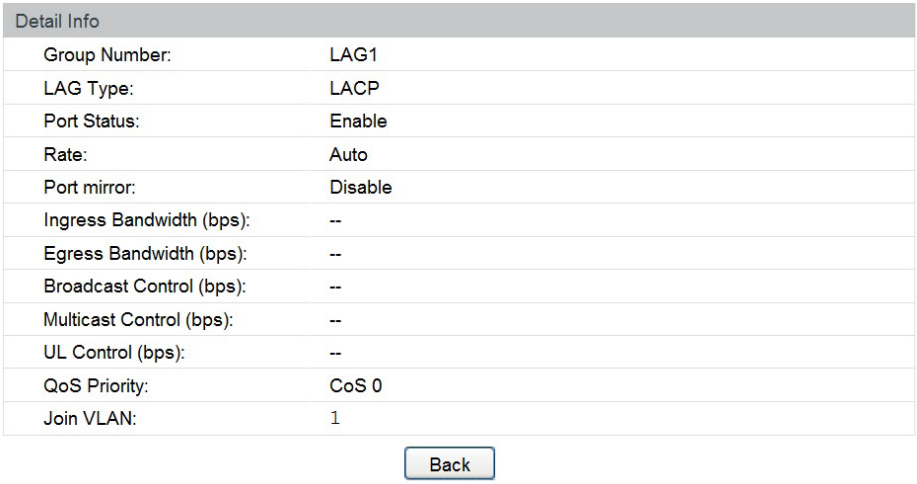
  Description: exibe a descrição do grupo LAG.

Member: exibe as portas membros do grupo LAG.

Operation: permite visualizar informações detalhadas ou modificar as configurações de cada grupo LAG.

» **Edit:** clique em *Edit* para modificar as configurações do grupo LAG desejado.

» **Detail:** clique em *Detail* para exibir informações detalhadas do grupo LAG desejado.

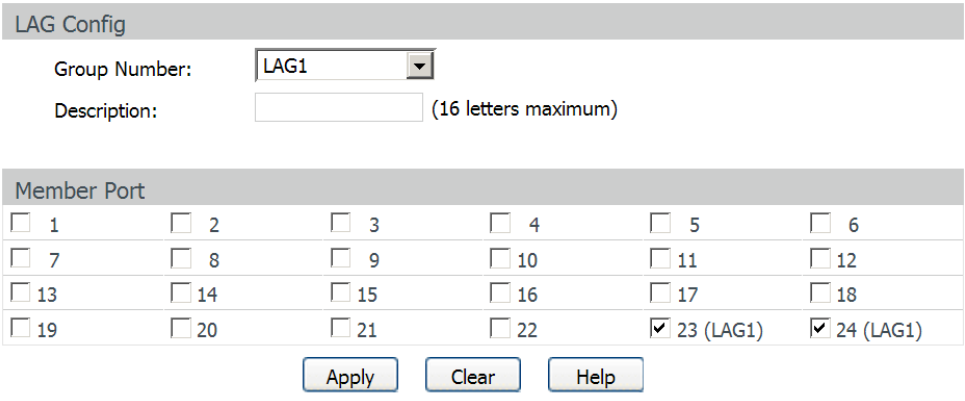


Detalhes do grupo LAG

Static LAG

Nesta página é possível configurar grupos LAGs Estáticos. O recurso LACP estará desabilitado para as portas membros de grupos LAGs Estáticos.

Escolha no menu *Switch* → *LAG* → *Static LAG* para carregar a seguinte página:


LAG Config
Group Number: LAG1
Description: (16 letters maximum)
Member Port
1 2 3 4 5 6
7 8 9 10 11 12
13 14 15 16 17 18
19 20 21 22 23 (LAG1) 24 (LAG1)
Apply Clear Help

Note:

1. LAG* denotes the Link Aggregation Group which the port belongs to.
2. It's not suggested to set 100M and 1000M ports in the same LAG.
3. The LAG created by LACP can't be modified.

Agregação de link estática

As seguintes informações são exibidas na tela:

» **LAG config**

Group number: selecione o número do grupo LAG.

Description: digite uma descrição para o grupo LAG.

» **LAG Table**

Member port: selecione as portas que participarão do grupo LAG. Para remover um grupo LAG, selecione todas as portas participantes do grupo e clique no botão *Clear*.

Obs.: *uma porta somente poderá participar de um grupo LAG. Se a porta já é membro de um grupo LAG ou se está configurado para um grupo de agregação dinâmica (LACP) a porta terá seu número exibido em cinza e não poderá ser selecionada.*

LACP config

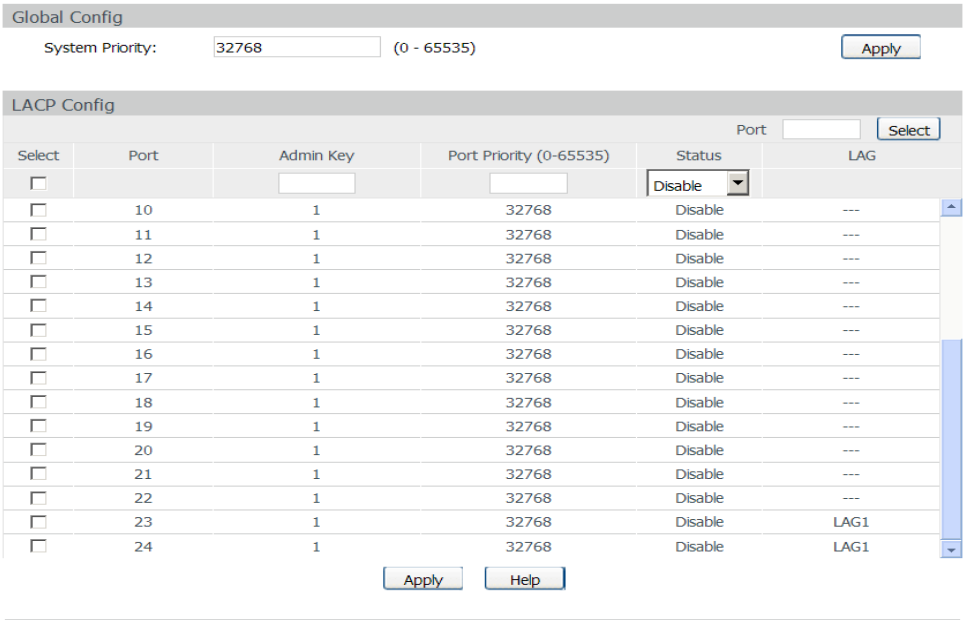
LACP (Link Aggregation Control Protocol) é definida pela norma IEEE802.3ad, e permite a agregação e desagregação de link de forma dinâmica, realizado através de trocas de pacotes LACP. Com o recurso LACP ativado, o switch enviará pacotes contendo a identificação da agregação de link (ID) para o seu parceiro e outras informações como Prioridade, endereço MAC do switch e Chave Administrativa. Uma agregação de link dinâmica, somente será realizada entre portas de switches com o mesmo ID de agregação de link.

Pode se formar até catorze grupos de agregação de link no switch. Se a quantidade configurada de grupos de agregação exceder o número máximo, o grupo que possuir o menor valor em "System Priority" terá prioridade na realização da agregação de link.

Do mesmo modo, até oito portas podem ser selecionadas para um grupo de agregação, portanto, a porta também possui uma prioridade para ser selecionada como membro de um grupo de agregação de link dinâmico. A porta com menor valor em "Port Piority" terá prioridade para realizar a agregação. Se duas portas possuírem prioridades iguais, a porta de número mais baixo terá a preferência.

Nesta página você pode configurar a função LACP para o switch.

Escolha o menu *Switching* → *LACP* → *LACP Config* para carregar a seguinte página:


Global Config
System Priority: 32768 (0 - 65535) Apply
LACP Config
Port Select
Select Port Admin Key Port Priority (0-65535) Status LAG
Disable
10 1 32768 Disable ---
11 1 32768 Disable ---
12 1 32768 Disable ---
13 1 32768 Disable ---
14 1 32768 Disable ---
15 1 32768 Disable ---
16 1 32768 Disable ---
17 1 32768 Disable ---
18 1 32768 Disable ---
19 1 32768 Disable ---
20 1 32768 Disable ---
21 1 32768 Disable ---
22 1 32768 Disable ---
23 1 32768 Disable LAG1
24 1 32768 Disable LAG1
Apply Help

Note:

1. To avoid any broadcast storm when LACP takes effect, you are suggested to enable Spanning Tree function.
2. LACP function can't be enabled for the port already in a static link aggregation group.

As seguintes informações são exibidas na tela:

» **Global config**

System Priority: digite o valor para a Prioridade do Sistema LACP. A prioridade do sistema combinado com o endereço MAC do switch constituem o ID de agregação. A agregação dinâmica somente será formada com grupos de agregação contendo o mesmo ID de agregação.

» **LACP config**

Port: digite o número da porta desejada dentro do campo correspondente e clique no botão *Select* para selecionar a porta.

Select: selecione a porta desejada para configuração LACP. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Admin key: especifique o valor da chave administrativa para a porta. Esta opção define a capacidade de agregação entre as portas. As portas membros da agregação dinâmica devem possuir a mesma chave de admin.

Port priority: especifique o valor para o Port Priority. É possível configurar a priorização de portas que pertencem ao mesmo grupo de agregação dinâmica. A porta com menor valor em "Port Priority" terá maior prioridade para realizar a agregação. Se duas portas possuírem prioridades iguais, a porta de número mais baixo terá a preferência.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a função LACP para a porta desejada.

LAG: exibe o número do grupo LAG a qual a porta pertence.

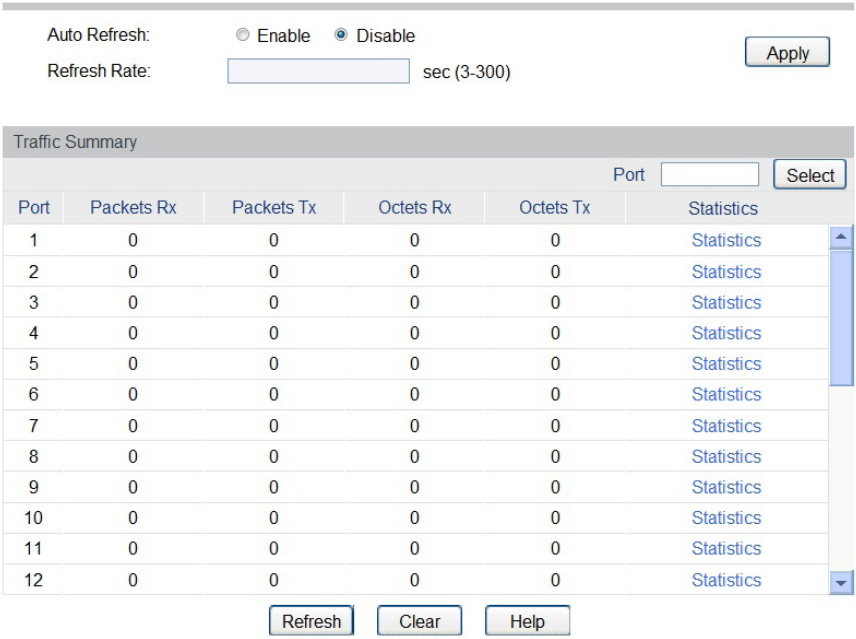
5.3. Traffic monitor

No sub-menu Traffic Monitor é possível monitorar e visualizar informações detalhadas do tráfego em cada porta do switch através das páginas *Traffic Summary* e *Traffic Statistics*.

Traffic summary

A página Traffic Summary exibe informações do tráfego em cada porta, o que facilita o monitoramento do tráfego da rede como um todo.

Escolha no menu *Switching* → *Traffic Monitor* → *Traffic Summary* para carregar a seguinte página:



Informações do tráfego

As seguintes informações são exibidas na tela:

» **Auto refresh**

Auto refresh: selecione *Enable/Disable* para habilitar ou desabilitar a atualização automática da página Traffic Summary.

Refresh date: digite o valor do intervalo (em segundos) de atualização da página Traffic Summary. O valor pode variar de 3 a 300 segundos.

» **Traffic summary**

Port select: digite o número da porta desejada dentro do campo correspondente e clique no botão *Select* para selecionar a porta.

Port: exibe o número da porta.

Packets RX: exibe o número de pacotes recebidos pela porta. Os pacotes com erro não participam desta estatística.

Packets TX: exibe o número de pacotes transmitidos pela porta.

Octets RX: exibe o número de bytes recebidos pela porta.

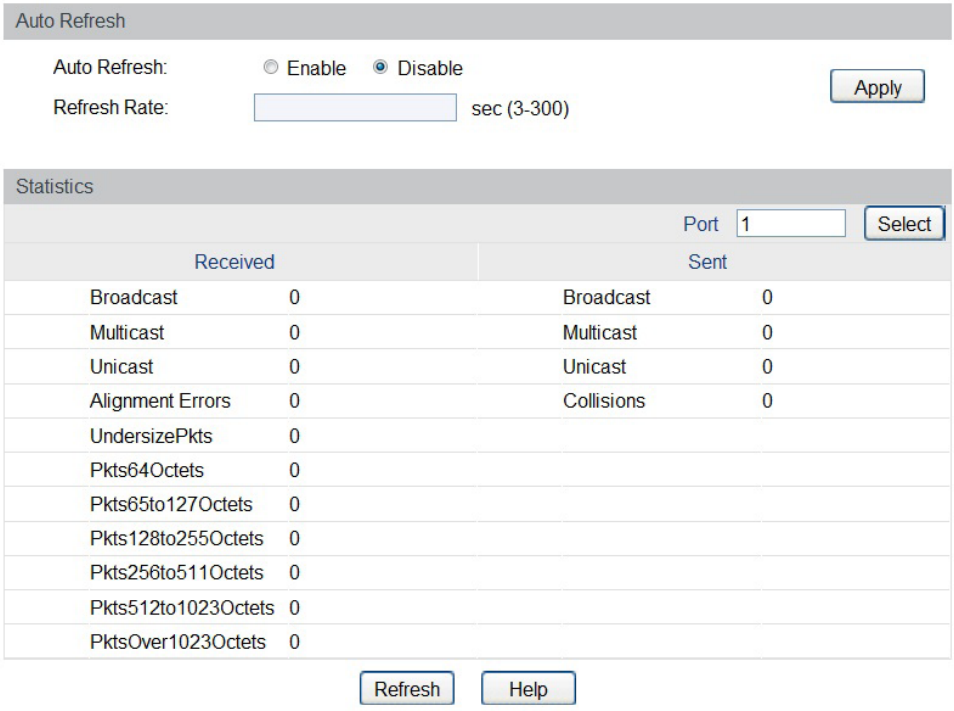
Octets TX: exibe o número de bytes transmitidos pela porta.

Statistics: clique em *Statistics* para visualizar as estatísticas detalhadas dos pacotes recebidos pela porta.

Traffic statistics

A página Traffic Statistics exibe as informações detalhadas do tráfego em cada porta, o que pode facilitar o monitoramento do tráfego da rede e localizar falhas rapidamente.

Escolha no menu *Switiching* → *Traffic Monitor* → *Traffic Statistics* para carregar a seguinte página:



Estatísticas do tráfego

As seguintes informações serão exibidas:

» **Auto refresh**

Auto refresh: selecione *Enable/Disable* para habilitar ou desabilitar a atualização automática da página Traffic Statistics.

Refresh date: digite o valor do intervalo (em segundos) de atualização da página Traffic Statistics. O valor pode variar de 3 a 300 segundos.

» **Statistics**

Port: digite o número da porta desejada dentro do campo correspondente e clique no botão *Select* para selecionar a porta.

Received: exibe os detalhes dos pacotes recebidos pela porta selecionada.

Sent: exibe os detalhes dos pacotes enviados pela porta selecionada.

Broadcast: exibe o número de pacotes broadcast transmitidos ou recebidos na porta selecionada. Os pacotes com erros não são contabilizados nesta página.

Multicast: exibe o número de pacotes Multicast transmitidos ou recebidos na porta selecionada. Os pacotes com erros não são contabilizados nesta página.

Unicast: exibe o número de pacotes unicast transmitidos ou recebidos na porta selecionada. Os pacotes com erros não são contabilizados nesta página.

Alignment errors: exibe o número dos pacotes recebidos que possuam erros de FCS (frame Check Sequence) ocasionados por erros nos bytes recebidos (Alignment Errors). O comprimento dos pacotes deverão possuir entre 64 e 1518 bytes de tamanho.

UndersizePkts: exibe o número de pacotes recebidos menores que 64 bytes (pacotes com erros não são contabilizados).

Pkts64Octets: exibe o número de pacotes recebidos iguais a 64 bytes (pacotes com erros não são contabilizados).

Pkts65to127Octets: exibe o número de pacotes recebidos que possuem comprimento entre 65 e 127 bytes (pacotes com erros não são contabilizados).

Pkts128to255Octets: exibe o número de pacotes recebidos que possuem comprimento entre 128 e 255 bytes (pacotes com erros não são contabilizados).

Pkts256to511Octets: exibe o número de pacotes recebidos que possuem comprimento entre 256 e 511 bytes (pacotes com erros não são contabilizados).

Pkts512to1023Octets: exibe o número de pacotes recebidos que possuem comprimento entre 512 e 1023 bytes (pacotes com erros não são contabilizados).

PktsOver1023Octets: exibe o número de pacotes recebidos maiores que 1023 bytes (pacotes com erros não são contabilizados).

Collisions: exibe o número de colisões detectadas em uma porta durante a transmissão de pacotes.

5.4. MAC address

Quando um equipamento de rede é conectado a uma das portas do switch, este aprende o endereço MAC do dispositivo e cria uma associação entre o endereço MAC e o número da porta, criando uma entrada na tabela de encaminhamento (Tabela de endereços MAC). Esta tabela é a base para que o switch possa encaminhar os pacotes rapidamente, entre o endereço de origem e destino, diminuindo o tráfego em broadcast. Os endereços MAC são adicionados na tabela de endereços de forma dinâmica (auto-aprendizagem) ou configurado manualmente.

Existem recursos de filtragem de endereços MAC, permitindo que o switch filtre pacotes indesejados, proibindo seu encaminhamento e melhorando a segurança da rede.

Características da tabela de endereços MAC.

Modo de entrada dos endereços na Tabela de endereços MAC	Modo de configuração	As entradas da Tabela de endereço MAC possui tempo de envelhecimento (aging time)	A Tabela de endereços MAC é mantida após reiniciar o switch (se a configuração for salva).	Relação entre o endereço MAC e a porta do switch.
Endereços Estáticos	Configuração Manual	Não	Sim	O endereço MAC aprendido por uma porta não pode ser aprendido por outra porta em uma mesma VLAN.
Endereços Dinâmicos	Aprendizado automático	Sim	Não	O endereço MAC aprendido por uma porta pode ser aprendido por outra porta em uma mesma VLAN.
Filtro de endereços	Configuração Manual	Não	Sim	-

O sub-menu MAC Address possui as seguintes páginas de configuração: *Address Table, Static Address, Dynamic Address* e *Filtering Address.*

Address table

Nesta página, você poderá visualizar as informações da Tabela de endereços MAC.

Escolha no menu *Switching* → *MAC Address* → *Address Table* para carregar a seguinte página:

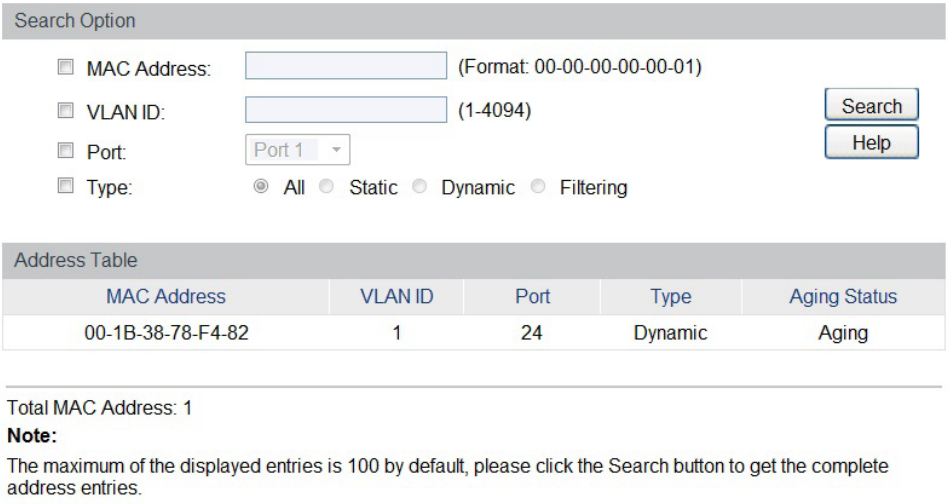


Tabela de endereço MAC

As seguintes informações são exibidas na tela:

» **Search option**

MAC address: digite o endereço MAC para filtrar os resultados desejados e clique em *Search*. Utilize o formato: 00-00-00-00-00-01.

VLAN ID: digite a VLAN ID para filtrar os resultados de acordo com a VLAN desejada e clique em *Search*.

Port: selecione o número da porta desejado para visualizar as entradas correspondentes e clique em *Search*.

Type: selecione o tipo de entrada desejado para filtrar os endereços MAC.

» **All:** esta opção exibe todas as entradas da Tabela de endereços MAC.

» **Static:** esta opção exibe todas as entradas estáticas da Tabela de endereços MAC.

» **Dynamic:** esta opção exibe todas as entradas dinâmicas da Tabela de endereços MAC.

» **Filtering:** esta opção exibe todos os endereços filtrados da Tabela de endereços MAC.

» **Address table**

MAC address: exibe o endereço MAC aprendido pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC.

Port: exibe o número da porta que está vinculado ao endereço MAC.

Type: exibe o modo de aprendizagem dos endereços MAC.

Aging status: exibe se a entrada possui ou não tempo de envelhecimento (aging time).

Static address

Nesta página é possível configurar entradas estáticas na Tabela de endereços MAC. As entradas estáticas somente podem ser adicionadas ou removidas manualmente, independentemente do tempo de envelhecimento da entrada (aging time).

Em redes estáveis, as entradas de endereços MAC estático pode aumentar consideravelmente o desempenho de encaminhamento de pacotes do switch. O endereço MAC estático aprendido com Port Security ativo será exibido na Tabela de endereços MAC.

Escolha o menu *Switching* → *MAC Address* → *Static Address* para carregar a seguinte página:

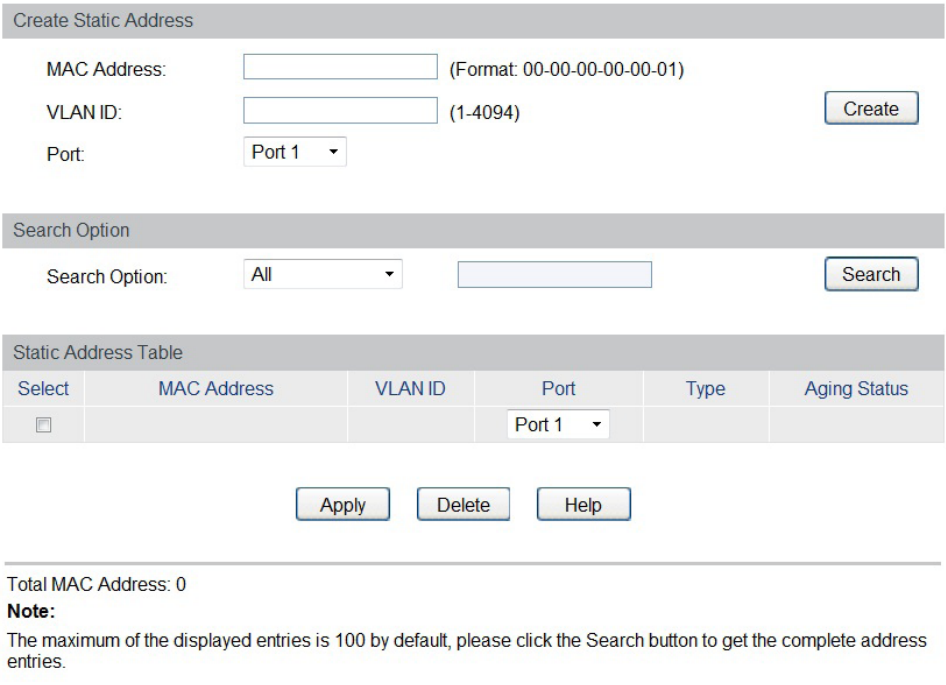


Tabela de endereços MAC estáticos

As seguintes mensagens são exibidas na tela:

» **Create static address**

MAC address: digite o endereço MAC que será adicionado a Tabela de endereços MAC, utilize o formato: 00-00-00-00-00-01 e clique no botão *Create* (é necessário preencher os campos *VLAN ID e Port* para validar a entrada).

VLAN ID: digite a VLAN ID que será associada ao endereço MAC que será adicionado a Tabela de endereços MAC.

Port: selecione a porta que será atrelada ao endereço MAC que será adicionado a Tabela de endereço MAC.

» **Search option**

Search option: selecione o modo de pesquisa e clique no botão *Search*, para encontrar a entrada estática na Tabela de endereços MAC.

» **MAC:** digite o endereço MAC para sua pesquisa.

» **VLAN ID:** digite o número da VLAN ID para sua pesquisa.

» **Port:** digite o número da porta para sua pesquisa.

» **Static address table**

Select: selecione a entrada desejada para remover da Tabela de endereços MAC clicando em *Delete* ou para modificar a porta correspondente que a entrada pertence selecionando uma nova porta.

MAC address: exibe o endereço MAC aprendido pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC.

Port: exibe o número da porta que está vinculado ao endereço MAC.

Type: exibe o modo de aprendizagem dos endereços MAC.

Aging status: exibe se a entrada possui ou não tempo de envelhecimento (aging time).

Obs.: » *Se o endereço MAC configurado para a porta correspondente estiver errado, ou o dispositivo conectado a porta for alterado, o switch não realizará o encaminhamento de pacotes. Por favor, redefina as entradas de endereço MAC de forma adequada.*

» *Se o endereço MAC de um dispositivo for configurado para uma porta e o dispositivo for conectado em outra porta, o switch não reconhecerá o endereço MAC dinamicamente. Portanto certifique-se que as entradas na Tabela de endereços MAC sejam válidas e corretas.*

» *Os endereços MAC configurados estaticamente não podem ser adicionados na tabela de endereços filtrados, ou vinculados a uma porta de forma dinâmica.*

Dynamic address

As entradas de endereços MAC realizadas de forma dinâmica são geradas pelo mecanismo de auto-aprendizagem do switch, através deste recurso, juntamente com o recurso de tempo de envelhecimento (aging time) são responsáveis pela manutenção da Tabela de endereços MAC.

O Aging Time faz com que o switch remova cada entrada da Tabela de endereços MAC dentro de um determinado período de tempo (tempo de envelhecimento) em que a entrada permanecer ociosa dentro da Tabela de endereços MAC.

Nesta página você pode configurar os endereços MAC dinâmico.

Escolha o menu *Switching* → *MAC Address* → *Dynamic Address* para carregar a seguinte página:

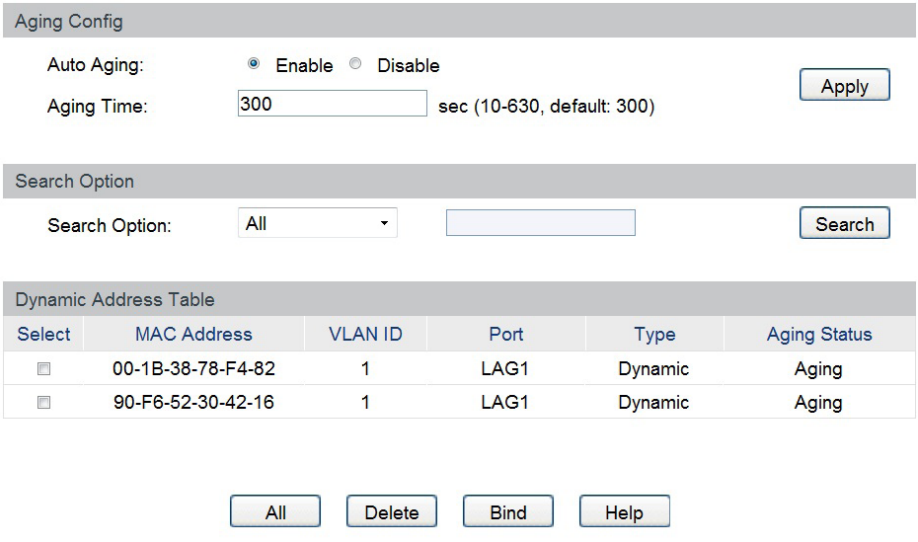


Tabela de endereços MAC dinâmica

As seguintes opções são exibidas na tela:

» **Aging config**

Auto aging: selecione *Enable/Disable* para habilitar ou desabilitar o recurso de tempo de envelhecimento (aging time) de uma entrada na Tabela de endereços MAC.

Aging time: digite o valor do intervalo (em segundos) do tempo de envelhecimento (aging time) de uma entrada na Tabela de endereços MAC. O valor pode variar de 10 a 630 segundos, por padrão este valor é de 300 segundos.

» **Search option**

Search option: selecione o modo de pesquisa e clique no botão *Search*, para encontrar a entrada dinâmica na Tabela de endereços MAC.

- » **ALL:** esta opção exibe todas as entradas dinâmicas da Tabela de endereços MAC.
- » **MAC address:** digite o endereço MAC para sua pesquisa.
- » **VLAN ID:** digite o número da VLAN ID para sua pesquisa.
- » **Port:** digite o número da porta para sua pesquisa

» **Dynamic address table**

Select: selecione a entrada desejada para remover da Tabela de endereços MAC clicando em *Delete* ou para vincular a entrada a uma porta de forma estática clicando em *Bind*.

MAC address: exibe o endereço MAC aprendido pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC.

Port: exibe o número da porta que está vinculado ao endereço MAC.

Type: exibe o modo de aprendizagem dos endereços MAC.

Aging status: exibe se a entrada possui ou não tempo de envelhecimento (aging time).

Bind: clique no botão *Bind* para vincular o endereço MAC a uma porta de forma estática.

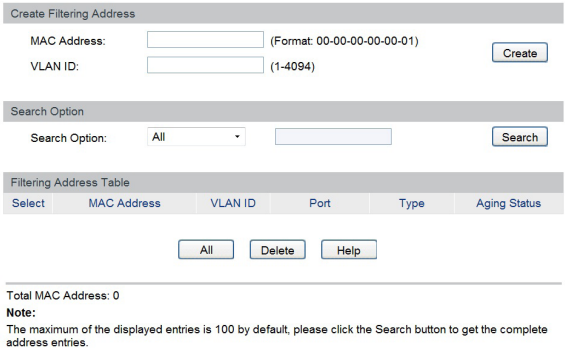
Obs.: *se o tempo de envelhecimento (aging time) do endereço MAC for muito longo ou muito curto poderá resultar em perda de desempenho do switch. Se o tempo for muito longo, poderá ocorrer o esgotamento da Tabela de endereços MAC, por estar com excesso de endereços MAC, o switch não aprenderá novos endereços, impedindo que as tabelas se atualizem com as mudanças ocorridas na rede. Se o tempo for muito curto, o switch poderá remover endereços MAC válidos, isso fará com que o switch tenha que aprender várias vezes o mesmo endereço MAC, ocasionando uma perda de desempenho. Recomenda-se que mantenha o valor padrão.*

Filtering address

A filtragem de endereços MAC, proíbe que pacotes indesejáveis sejam encaminhados pelo switch. Os endereços para filtragem podem ser adicionados ou removidos manualmente, independente do tempo de envelhecimento (aging time) do endereço MAC.

A filtragem de endereços MAC permite que o switch filtre os pacotes que incluem o endereço MAC especificado, como endereço de origem ou destino, de modo a garantir a segurança da rede. As regras de filtragem de endereços MAC atuarão na VLAN correspondente.

Escolha no menu *Switching* → *MAC Address* → *Filtering Address* para carregar a seguinte página:



Filtro de endereço MAC

As seguintes informações são exibidas:

» **Create filtering address**

MAC address: digite o endereço MAC que será filtrado, proibindo a sua inclusão na Tabela de endereços MAC, utilize o formato: 00-00-00-00-00-01 e clique em *Create* (é necessário preencher o campo *VLAN ID* para validar a entrada).

VLAN ID: digite a VLAN ID que será atrelada ao endereço MAC que será filtrado na Tabela de endereços MAC.

» **Search option**

Search option: selecione o modo de pesquisa e clique no botão *Search*, para encontrar o filtro desejado na Tabela de endereços MAC.

» **MAC address:** digite o endereço MAC para sua pesquisa.

» **VLAN ID:** digite o número da VLAN ID para sua pesquisa.

» **Filtering address table**

Select: selecione a entrada desejada para remover o filtro correspondente da Tabela de endereços MAC, clicando em *Delete*.

MAC address: exibe o endereço MAC que será filtrado pelo switch.

VLAN ID: exibe a VLAN ID que está vinculada ao endereço MAC filtrado.

Port: exibe o número da porta que está vinculado ao endereço MAC filtrado.

Type: exibe o modo de aprendizagem dos endereços MAC.

Aging status: exibe se a entrada possui ou não tempo de envelhecimento (aging time).

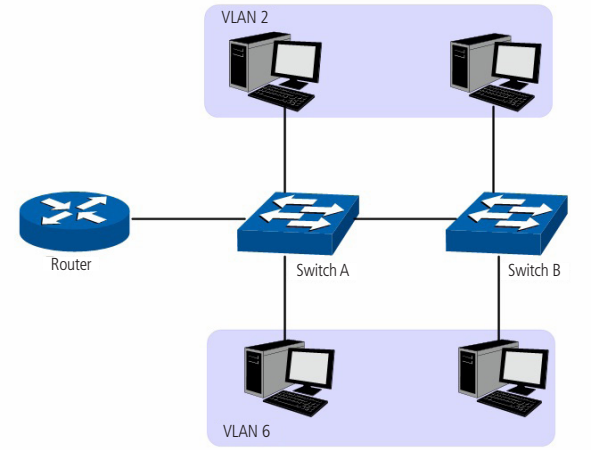
Obs.: » *Os endereços MAC filtrados não poderão ser inclusos na Tabela de endereços MAC, utilizando os recursos de modo estático ou dinâmico.*

» *O recurso de filtro de endereços MAC não estará disponível se a função 802.1X estiver habilitada.*

6. VLAN

VLAN (Virtual Local Area Network) é o modo que torna possível dividir um único segmento de rede "LAN" em vários segmentos lógicos "VLAN".

Cada VLAN se torna um domínio de broadcast, evitando assim a inundação de pacotes broadcast, otimizando a performance do switch, além facilitar o gerenciamento e segurança da rede. Para haver comunicação entre computadores em VLANs diferentes é necessária a utilização de roteadores ou switch layer 3 para o encaminhamento dos pacotes. A figura a seguir ilustra uma implementação de VLAN.



VLAN

Principais vantagens na utilização de VLAN:

1. As transmissões em broadcast estão restritas a cada VLAN. Isso diminui a utilização de banda e melhora o desempenho da rede.
2. Melhoria na segurança da rede: VLANs não podem se comunicar umas com as outras diretamente, ou seja, um computador em uma VLAN não pode acessar os recursos contidos em outra VLAN, a menos que seja utilizado um roteador ou switch camada 3 para realizar esta comunicação.
3. Flexibilidade na alteração de layout: é possível ter computadores separados geograficamente (por exemplo, computadores em andares diferentes) pertencerem à mesma VLAN sem a necessidade de alteração física da topologia da rede.

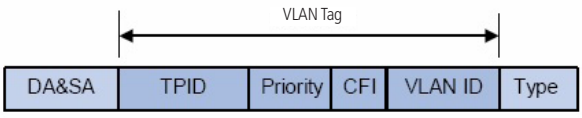
Este switch suporta três modos de classificação de VLAN: *802.1Q VLAN, MAC VLAN e Protocol VLAN.*

6.1. 802.1Q VLAN

As tags de VLANs são necessárias para o switch identificar os pacotes de diferentes VLANs. O switch trabalha na camada de enlace no modelo OSI, podendo desta forma, analisar e gerenciar os quadros que possuam a tag de VLAN.

Em 1999, o IEEE padronizou a aplicação 802.1Q VLAN, definindo uma estrutura de tags de VLAN nos quadros Ethernet. O protocolo IEEE802.1Q define que 4 bytes são adicionados ao quadro Ethernet (esta inserção ocorre logo após os campos de endereço MAC de destino e origem do frame Ethernet) para tornar possível a utilização de VLANs em redes Ethernet.

A figura a seguir, exibe quatro novos campos que o protocolo 802.1Q (tag de VLAN) adiciona ao frame Ethernet: TPID (Tag Protocol IDentifier), Priority, CFI (Canonical Format Indicator) e VLAN ID.



VLAN Tag

1. TPID: campo de 16 bits, indicando que a estrutura do frame é baseada em tag de VLAN, por padrão este valor é igual a 0x8100.
2. Priority: campo de 3 bits, referindo-se a prioridade 802.1p. Consulte o capítulo 9. QoS, para mais detalhes.
3. CFI: campo de 1 bit, indicando que o endereço MAC é encapsulado na forma canônica "0" ou não-canônica "1". Isso é utilizado no método de acesso ao meio roteados por FDDI/Token-Ring para sinalizar a ordem da informação de endereço encapsulado no quadro. Esse campo não é descrito em detalhes nesse manual.
4. VLAN ID: campo de 12 bits, que indentifica o VLAN ID (Identificação da VLAN) a qual o quadro pertence. Este intervalo varia entre 1 a 4094, normalmente os valores 0 e 4095 não são utilizados.

VLAN ID identifica a VLAN a qual o quadro pertence. Quando o switch recebe um pacote que não possui uma tag de VLAN (untagged), o switch irá encapsular o quadro com a tag de VLAN padrão da porta correspondente (PVID).

» **Modo de funcionamento das portas**

As portas do switch podem operar de três modos diferentes, a seguir a descrição de cada um dos modos:

1. **ACCESS:** a porta em modo ACCESS só pode ser adicionada em uma única VLAN, e a regra de saída da porta é UNTAG. O PVID é o mesmo que o ID de VLAN atual. Se a VLAN atual é excluida, o PVID será definido como 1 por padrão.
2. **TRUNK:** a porta em modo TRUNK pode ser adicionada em várias VLANs, e a regra de saída da porta é TAG. O PVID pode ser definido como o número VID de qualquer VLAN que a porta pertença.
3. **GENERAL:** a porta em modo GENERAL pode ser adicionada em várias VLANs e estabelecer regras de saídas diferentes de acordo com as diferentes VLANs. A regra de saída padrão é UNTAG. O PVID pode ser definido como o número VID de qualquer VLAN a qual a porta pertence.

» **PVID**

PVID (Port Vlan ID) é o VID (Identificação da VLAN) padrão da porta. Quando o switch recebe um pacote sem marcação (untagged), ele irá adicionar uma tag de VLAN no pacote de acordo com o PVID de sua porta. Ao criar VLANs, o PVID de cada porta indica a VLAN padrão a qual porta pertence. É um parâmetro importante com a seguinte finalidade.

1. Quando o switch recebe um pacote sem marcação (untagged), ele irá adicionar uma tag de VLAN no pacote de acordo com o PVID configurado em sua porta.
2. O PVID determina o domínio de broadcast padrão da porta, ou seja, quando a porta recebe pacotes de broadcast, a porta transmitirá os pacotes apenas para as portas do seu domínio de broadcast.

Pacotes marcados (tagged) ou não marcados (untagged) serão processados de maneiras diferentes, se recebidos por portas com diferentes modos de funcionamento. A tabela a seguir mostra como são tratados os pacotes.

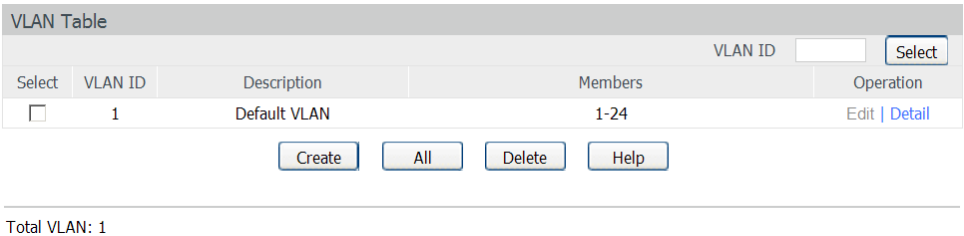
	Recebendo pacotes		
Tipo de Porta	**Pacotes UNTAG**	**Pacotes TAG**	**Enviando pacotes**
Access	Quando pacotes untagged são recebidos, a porta irá adicionar a TAG padrão da porta, isto é, o PVID da porta de entrada.	Se o VID de pacote é o mesmo que o PVID da porta, o pacote será recebido. Se o VID de pacote não é o mesmo que o PVID da porta, o pacote será descartado.	O pacote será enviado após retirar sua tag de VLAN.
Trunk		Se o VID do pacote é permitido pela porta, o pacote será recebido. Se o VID do pacote é proibido pela porta, o pacote será descartado.	O pacote será enviado com a sua tag de VLAN atual.
General			Se a regra de saída da porta é TAG, o pacote será enviado com a sua tag de VLAN atual. Se a regra de saída da porta é UNTAG, o pacote será enviado após retirar sua tag de VLAN.

A função IEEE802.1Q VLAN pode ser configurada nas páginas *VLAN Config* e *Port Config*.

VLAN config

Nesta página você poderá criar e visualizar as VLAN 802.1Q.

Escolha no menu *VLAN → 802.1Q VLAN → VLAN Config* para carregar a seguinte página.



Visualização das VLANs

Para garantir a comunicação com o switch, por padrão, a VLAN de Gerenciamento e todas as portas do switch estão configuradas na VLAN 1, sendo esta a única VLAN que não pode ser excluída.

As seguintes informações são exibidas na tela:

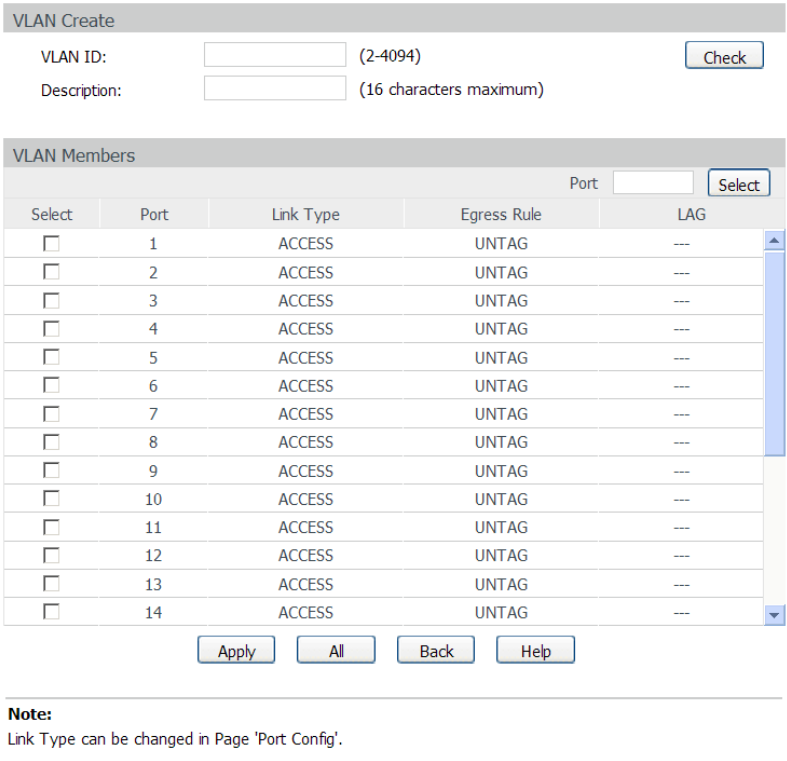
» **VLAN table**

VLAN ID: digite o VLAN ID desejado no campo correspondente e clique em *Select* para selecionar a VLAN desejada.
Select: selecione a VLAN desejada. Nesta opção é possível selecionar mais de uma VLAN simultaneamente.
VLAN ID: exibe o VLAN ID da VLAN (identificação da VLAN).
Description: exibe a descrição definida para a VLAN.
Members: exibe as portas membros da VLAN criada.
Operation: permite você visualizar ou modificar as informações de cada VLAN.

» **Edit:** clique em *Edit* para modificar as configurações da VLAN desejada.
» **Detail:** clique em *Detail* para visualizar as informações da VLAN desejada.

Create:

Ao clicar no botão *Create* ou *Edit* será exibido a tela de configuração de VLAN, conforme imagem a seguir.



Configuração de VLAN

As seguintes informações são exibidas na tela:

» **VLAN create**

VLAN ID: digite o ID de identificação da VLAN.

Description: digite uma descrição para a VLAN de no máximo 16 caracteres.

Check: clique no botão *Check* para verificar se o VLAN ID digitado é válido ou não.

» **VLAN members**

Port Select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número de porta.

Link type: exibe o modo de funcionamento da porta. Este campo é definido na página de configuração "Port Config".

Egress rule: exibe a regra de saída configurada para a porta. Se o modo de funcionamento da porta estiver configurado em General, será possível modificar esta opção.

» **TAG:** os pacotes transmitidos pela porta serão marcados (tagged – pacotes contendo informações de VLAN).

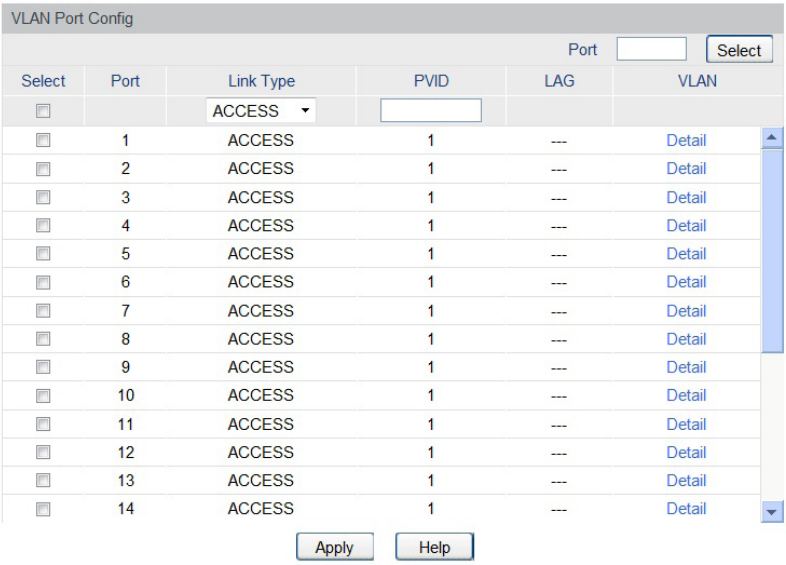
» **UNTAG:** os pacotes transmitidos pela porta não serão marcados (untagged).

LAG: exibe o número do grupo LAG a qual a porta pertence.

Port config

Nesta página é possível configurar e visualizar o modo de funcionamento das portas e seus respectivos PVID quando permitido.

Escolha no menu *VLAN → 802.1Q VLAN → Port Config* para carregar a página seguinte:



Modo de funcionamento das portas

As seguintes informações são exibidas:

» **VLAN port config**

Port select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Link type: selecione o modo de funcionamento da porta.

» **ACCESS:** a porta em modo ACCESS só pode ser adicionada em uma única VLAN, e a regra de saída da porta é UNTAG. O PVID é o mesmo que o ID de VLAN. Se a VLAN atual é excluída, o PVID será definido como 1 por padrão.

» **TRUNK:** a porta em modo TRUNK pode ser adicionada em várias VLANs, e a regra de saída da porta é TAG. O PVID pode ser definido como o número VID de qualquer VLAN que a porta pertença.

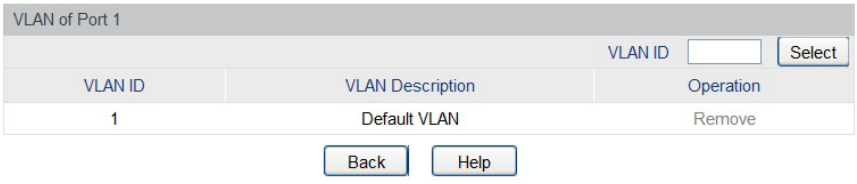
» **GENERAL:** a porta em modo GENERAL pode ser adicionada em várias VLANs e estabelecer regras de saídas diferentes de acordo com as diferentes VLANs. A regra de saída padrão é UNTAG. O PVID pode ser definido como o número VID de qualquer VLAN a qual a porta pertença.

PVID: digite o PVID a qual a porta pertence.

LAG: exibe o número do grupo LAG a qual a porta pertence.

VLAN: clique em *Detail* para exibir as informações da VLAN a qual a porta pertence.

Ao clicar em *Detail* serão exibidas as informações da VLAN da porta correspondente, conforme imagem a seguir:



Detalhes da VLAN (Porta 1)

As seguintes informações são exibidas na tela:

» **VLAN of port**

VLAN ID select: digite o VLAN ID desejado no campo correspondente e clique em *Select* para selecionar a VLAN.

VLAN ID: exibe o VLAN ID da VLAN (identificação da VLAN).

VLAN description: exibe a descrição definida para a VLAN.

Operation: permite remover a porta da VLAN atual.

Procedimento de configuração

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta.	Obrigatório, no menu VLAN ⟶ 802.1Q VLAN ⟶ Port Config, defina o modo de funcionamento da porta baseado no dispositivo conectado ao switch.
2	Criação da VLAN	Obrigatório, no menu VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config, clique no botão *Create* para criar a VLAN. Digite a VLAN ID e a descrição para a VLAN e especifique as portas membros da VLAN.
3	Modificar/Visualizar a VLAN	Opcional, no menu VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config clique no botão *Edit/Detail* para modificar ou visualizar as informações da VLAN correspondente.
4	Remover a VLAN	Opcional, no menu VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config, selecione a VLAN que deseja excluir e clique no botão *Remove*.

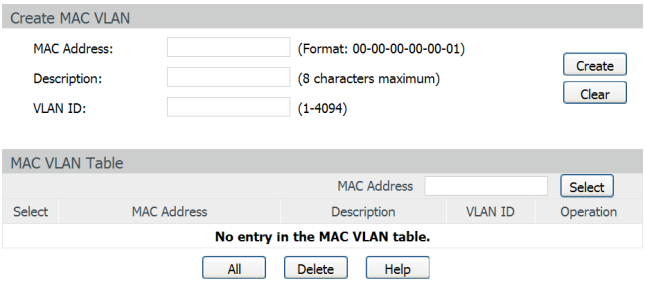
6.2. MAC VLAN

MAC VLAN é a maneira de classificar as VLANs de acordo com o endereço MAC dos dispositivos. Um endereço MAC corresponde a uma identificação de VLAN. Para um dispositivo que possua seu endereço MAC vinculado a uma VLAN poderá ser conectada a outras portas membros desta VLAN, que mesmo assim, terá seu papel de membro efetivo sem alterar as configurações de outros membros da VLAN.

Os pacotes de um MAC VLAN são processados da seguinte maneira:

1. Ao receber um pacote untagged, o switch verifica se o endereço MAC do pacote possui uma entrada correspondente nas configurações de MAC VLAN. Se o endereço MAC corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o VLAN ID do MAC VLAN configurado. Se o endereço MAC não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o PVID configurado para a porta. Assim o pacote será atribuído automaticamente para a VLAN correspondente.
2. Ao receber um pacote tagged, o switch irá processá-lo de acordo com as configurações 802.1Q VLAN. Se a porta que recebeu o pacote é membro da VLAN, o pacote será transmitido normalmente, caso contrário, o pacote será descartado.
3. Ao criar um MAC VLAN é necessário habilitar a porta para ser membro da VLAN 802.1Q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Escolha no menu VLAN ⟶ MAC VLAN para carregar a seguinte página.



Configuração do MAC

Nesta página, você pode criar e visualizar as configurações atuais do MAC VLAN.

As seguintes informações são exibidas na tela.

» **Create MAC VLAN**

MAC Address: digite o endereço MAC do dispositivo participante da MAC VLAN no formato: 00-00-00-00-00-01.

Description: digite uma descrição para a identificação do endereço MAC.

VLAN ID: digite a VLAN ID desejado para o MAC VLAN.

» **MAC VLAN Table**

MAC Address select: digite o endereço MAC desejado no campo correspondente e clique em *Select* para selecionar a entrada correspondente.

Select: selecione o MAC VLAN desejado. Nesta opção é possível selecionar mais de uma opção simultaneamente.

MAC Address: exibe o endereço MAC do dispositivo participante do MAC VLAN.

Description: exibe a descrição do MAC VLAN configurado.

VLAN ID: exibe o VLAN ID do endereço MAC corresponde.

Operation: clique em *Edit*, para modificar as configurações, após realizado as alterações, clique no botão *Modify* para aplicar as configurações.

Procedimento de configuração

Passos	Operação	Descrição
1	Definir o modo de funcionamento da porta.	Obrigatório, no menu VLAN ⟶ 802.1QVLAN ⟶ Port Config, defina o modo de funcionamento da porta baseado no dispositivo conectado ao switch.
2	Criar a VLAN	Obrigatório, no menu VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config, clique no botão Create para criar a VLAN. Digite o VLAN ID e a descrição para a VLAN e especifique as portas membros da VLAN.
3	Criar o MAC VLAN	Obrigatório, no menu VLAN ⟶ MAC VLAN, para criar o MAC VLAN. Digite o endereço MAC do dispositivo, a descrição e o VLAN ID utilizado pelo MAC VLAN. Ao criar um MAC VLAN é necessário habilitar a porta para ser membro da VLAN 802.1Q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

6.3. Protocol VLAN

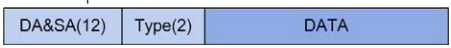
VLAN por Protocolo é a maneira de classificar as VLANs de acordo com o protocolo de rede utilizado, entre eles o IP, IPX, DECnet, AppleTalk, Banyan e assim por diante. Com a criação de VLANs por Protocolo, o administrador de rede pode gerenciar os clientes da rede baseando-se em suas aplicações e serviços de forma eficaz.

» **Formato de encapsulamento dos dados Ethernet**

Esta seção introduz a forma de encapsulamento comum dos dados Ethernet. Estes formatos são utilizados para a identificação de cada protocolo presente nos pacotes recebidos pelo switch.

Atualmente existem dois formatos de encapsulamento dos dados Ethernet. O encapsulamento Ethernet II e o encapsulamento 802.2/802.3, conforme mostrado a seguir:

» Encapsulamento Ethernet II



» Encapsulamento 802.2/802.3

DA e SA, referem-se respectivamente ao endereço MAC de destino e o endereço MAC de origem. O número informado entre parênteses indica o tamanho do campo em bytes.

O tamanho máximo de um frame Ethernet é de 1500 bytes, representado por 0x05DC em hexadecimal. O campo Length utilizado pelo encapsulamento 802.2/802.3 permite valores entre 0x0000 e 0x05DC (0 a 1500) e o campo Type utilizado pelo encapsulamento Ethernet II permite valores entre 0x0600 e 0xFFF (1536 a 4095), sendo através destes dois campos que o switch identifica o tipo de encapsulamento do frame Ethernet . Caso os campos Type e Length possuam valores entre 0x05DD a 0x05FF (1501 a 1535) o frame Ethernet é diretamente descartado, considerando o pacote como ilegal.

O encapsulamento 802.2/802.3 possui 3 possíveis formatos estendidos:

» Encapsulamento 802.3 Raw

Apenas o campo Length é encapsulado após o campo DA/SA (endereço MAC de destino e origem) seguido pelo campo DATA sem qualquer outro campo. Atualmente apenas o protocolo IPX suporta encapsulamento 802.3 Raw. Os dois últimos bytes do campo Length é 0xFFFF

» Encapsulamento 802.2 LLC (Logic Link Control)

DA&SA(12)	Length(2)	DSAP(1)	SSAP(1)	Control(1)	DATA

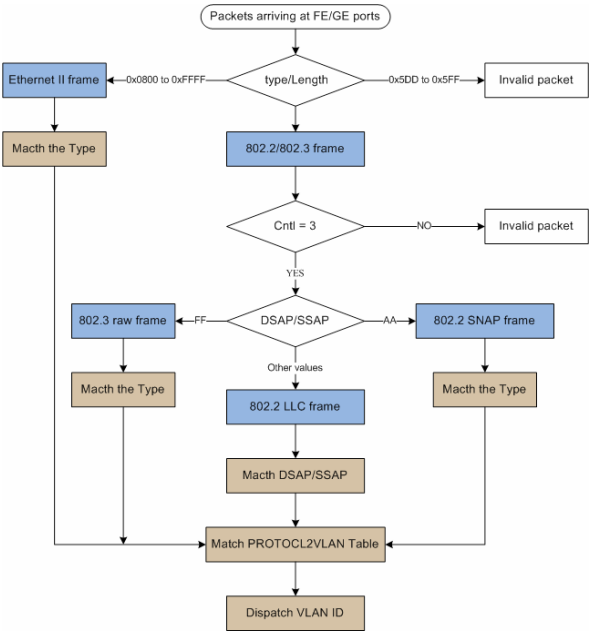
Apenas os campos Length, DSAP (Destination Service Access Point), SSAP (Source Service Access Point) e Control são encapsulados após o campo DA/SA (endereço MAC de destino e origem). O valor do campo Control é sempre 3. Os campos DSAP e SSAP do encapsulamento 802.2 LLC são utilizados para identificar o protocolo da camada superior, por exemplo, quando os dois campos possuem os valores 0xE0, indica que o protocolo da camada superior é o IPX.

» Encapsulamento 802.2 SNAP (Sub-Network Access Protocol)

No encapsulamento 802.2 SNAP os valores dos campos DSAP e SSAP são sempre 0xAA e o valor do campo Control é 3. O switch diferencia os encapsulamentos 802.2 LLC e SNAP de acordo com os valores dos campos DSAP e SSAP.

O dispositivo determina a forma de encapsulamento dos pacotes enviados. Um dispositivo pode enviar pacotes com os dois formatos de encapsulamento. O encapsulamento Ethernet II é o mais utilizado atualmente.

» **Procedimento de identificação do pacote pelo switch.**



Identificação do encapsulamento Ethernet

» **Implementação da VLAN por Protocolo**

No switch é possível criar modelos de protocolos para transmitir os pacotes correspondentes nas VLANs desejadas. Modelos de protocolos compreendem a forma de encapsulamento e o tipo de protocolo, determinando desta forma, o protocolo de rede utilizado pelo pacote.

A seguinte tabela mostra os formatos comuns de encapsulamento suportados pelos protocolos de rede utilizados pela camada de rede. O switch possui alguns modelos de protocolos pré-determinados, sendo possível adicionar outros modelos conforme sua necessidade.

	Encapsulamento			
Protocolo	**Ethernet II**	**802.3 Raw**	**802.2 LLC**	**802.2 SNAP**
IP (0x0800)	Suportado	Sem suporte	Sem suporte	Suportado
IPX (0x8137)	Suportado	Suportado	Suportado	Suportado
AppleTalk (0x809B)	Suportado	Sem suporte	Sem suporte	Suportado

» **Os pacotes em uma VLAN por Protocolo são processados da seguinte maneira:**

1. Ao receber um pacote untagged, o switch verifica se o protocolo de rede do pacote possui uma entrada correspondente nas configurações de VLAN por Protocolo. Se o protocolo de rede corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o VLAN ID da VLAN por Protocolo configurado. Se o protocolo de rede não corresponder, o switch adicionará a tag de VLAN no pacote de acordo com o PVID configurado para a porta. Assim o pacote é atribuido automaticamente para a VLAN correspondente.
2. Ao receber um pacote tagged, o swtich irá processá-lo de acordo com as configurações 802.1Q VLAN. Se a porta que recebeu o pacote é membro da VLAN, o pacote será trasmitido normalmente, caso contrário, o pacote sera descartado.
3. Ao criar VLANs por Protocolo, é necessário habilitar a porta para ser membro da VLAN 802.1Q correspondente, de modo a garantir que os pacotes sejam encaminhados normalmente.

Protocol Group Table

Nesta página é possível criar VLANs por Protocolo clicando no botão *Create* ou visualizar as informações das atuais VLANs por Protocolos já definidas.

Escolha no menu VLAN ⟶ Protocol VLAN ⟶ Protocol Group Table para carregar a seguinte página.

Tabela das VLANs por Protocolo

As seguintes informações são exibidas.

» **Protocol Group Table**

Select: selecione a VLAN por Protocolo desejada. Nesta opção é possível selecionar mais de uma entrada simultaneamente.

Protocol: exibe o nome do protocolo de rede configurado para a VLAN por Protocolo.

VLAN ID: exibe o VLAN ID (identificação de VLAN) correspondente ao protocolo de rede.

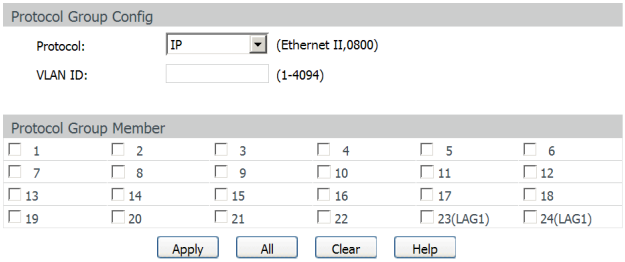
Member: exibe as portas membros da VLAN por Protocolo.

Operation: clique em *Edit* para modificar as configurações das VLANs por Protocolo. Após realizado as modificações, clique em *Apply* para aplicar as mudanças.

Protocol Group

Nesta página é possível criar VLANs por Protocolo de acordo com os protocolos pré-definidos pelo switch ou com os modelos de protocolos previamente configurados. O switch possui os seguintes modelos de protocolos por padrão: IP, ARP, RARP, IPX e AT.

Escolha no menu VLAN ⟶ Protocol VLAN ⟶ Protocol Group para carregar a seguinte página.



Criação de VLAN por Protocolo

As seguintes informações são apresentadas na tela.

» **Protocol Group Config**

Protocol: selecione o protocolo de rede utilizado pela VLAN por Protocolo.

VLAN ID: digite a VLAN ID (identificação de VLAN) da VLAN por Protocolo.

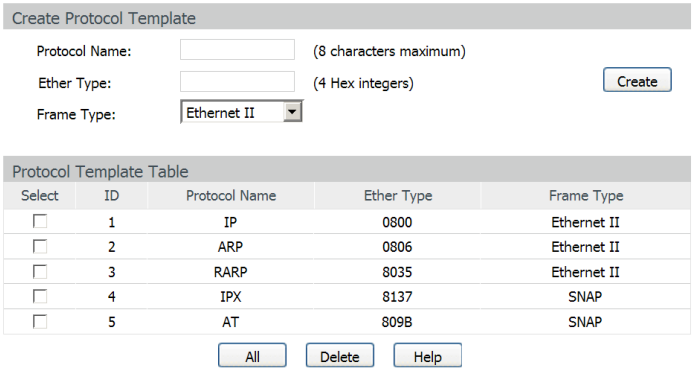
» **Protocol Group Member**

Selecione as portas habilitadas para a VLAN por Protocolo. Todas as portas estão desabilitadas por padrão. Nesta opção é possível selecionar mais de uma entrada simultaneamente.

Protocol Template

Esta página é utilizada para criar os modelos de protocolos desejados. Os modelos de protocolo devem ser criados antes de configurar a VLAN por Protocolo. O switch por padrão tem definidos os seguintes modelos de protocolos: IP, ARP, RARP, IPX, AT.

Escolha no menu VLAN → Protocol VLAN → Protocol Template para carregar a seguinte página.



Criação e visualização dos modelos de protocolos

As seguintes informações são exibidas na tela.

» **Create Protcol Template**

Protocol Name: digite o nome para o modelo de protocolo que será criado. Este campo deve possuir no máximo 8 caracteres.

Ether Type: digite a valor em hexadecimal referente ao tipo de protocolo de rede desejado.

Frame Type: selecione o tipo de encapsulamento utilizado pelo modelo de protocolo.

» **Protocol Template Table**

Select: selecione o modelo de protocolo desejado. Nesta opção é possível selecionar mais de um modelo simultaneamente.

ID: exibe o índice do modelo de protocolo.

Protocol Name: exibe o nome do modelo de protocolo criado.

Ether Type: exibe as informações do protocolo de rede utilizado pelo modelo.

Frame Type: exibe informações sobre o tipo de encapsulamento utilizado pelo quadro Ethernet .

Obs.: *não é possível remover um modelo de protocolo quando este modelo está vinculado a uma VLAN.*

Procedimento de configuração

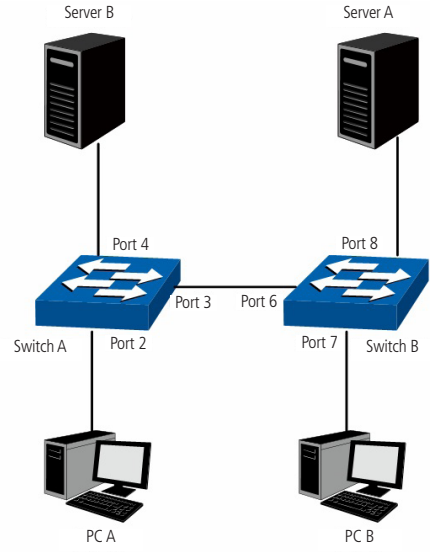
Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Port Config, defina o modo de funcionamento da porta baseado no dispositivo conectado ao switch.
2	Criação da VLAN	Obrigatório, VLAN → 802.1Q VLAN → VLAN Config, clique no botão *Create* para criar a VLAN. Entre com a VLAN ID e a descrição para a VLAN.
3	Criação do Modelo de Protocolo	Obrigatório, VLAN → Protocol VLAN → Protocol Template, Defina o Modelo de Protocolo antes de configurar a VLAN por Protocolo.
4	Criação da VLAN por Protocolo	Obrigatório, VLAN → Protocol VLAN → Protocol Group, selecione o modelo de protocolo, a VLAN ID e as portas participantes da VLAN por Protocolo.
5	Modificação/Visualização da VLAN por Protocolo	Opcional, VLAN → Protocol VLAN → Protocol Group Table, clique em *Edit* para modificar ou visualizar a VLAN por Protocolo correspondente.
6	Remover a VLAN por Protocolo	Opcional, VLAN → Protocol VLAN → Protocol Group Table, selecione a VLAN por Protocolo desejada e clique no botão *Delete*.

6.4. Exemplos de aplicação para 802.1Q VLAN

» **Requisitos da rede**

- » O switch A está conectado ao PC A e Server B.
- » O switch B está conectado ao PC B e Server A.
- » O PC A e o Server A estão na mesma VLAN.
- » O PC B e o Server B estão na mesma VLAN.
- » Os PCs em VLANs diferentes não podem se comunicar uns com os outros.

» **Diagrama da rede**



Aplicação de VLAN 802.1Q

» **Procedimento de configuração**

» Configuração do switch A

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Port Config. Configurar o modo de funcionamento da porta 2, porta 3 e porta 4 como ACCESS, TRUNK e ACESS respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → VLAN config, criar a VLAN com o VLANID 10 nas portas 2 e 3.
3	Criar a VLAN 20	Obrigatório, VLAN → 802.1Q VLAN → VLAN Config. Criar a VLAN com o VLANID 20 nas portas 3 e 4.

» Configuração do switch B

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ Port Config. Configurar o modo de funcionamento da porta 7, porta 6 e porta 8 como ACCESS, TRUNK e ACESS respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config, criar VLAN com o VLANID 10 nas portas 6 e 8.
3	Criar a VLAN 20	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config. Criar a VLAN com o VLANID 20 nas portas 6 e 7.

6.5. Exemplos de aplicação para MAC VLAN

» **Requisitos de rede**

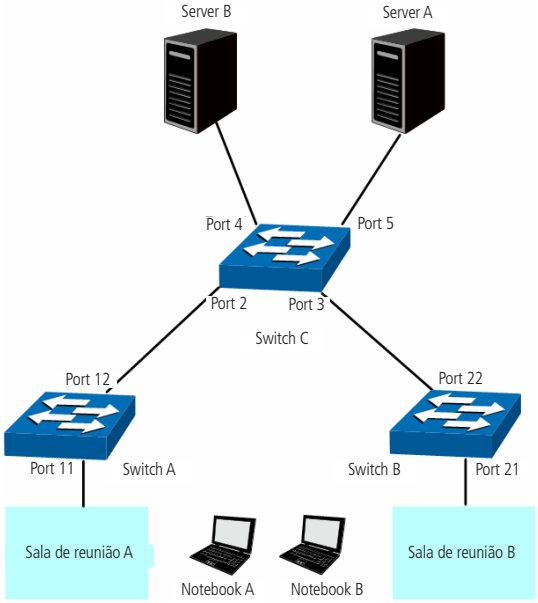
» O switch A e o switch B estão localizados respectivamente nas salas de reunião A e B, estas salas são utilizadas por todos os departamentos.

» O notebook A e o notebook B são utilizados em ambas as salas de reunião e possuem acesso a departamentos diferentes.

» Os dois departamentos estão respectivamente na VLAN 10 e VLAN 20, Os dois notebooks podem acessar tanto o servidor A e o servidor B de qualquer uma das salas de reunião, mesmo os servidores estando em VLANs distintas.

» O endereço MAC do notebook A é 00-19-56-8A-4C-71 e do notebook B é 00-19-56-82-3B-70.

» **Diagrama da rede**



Aplicação de MAC VLAN

» **Procedimento de configuração**

» Configuração do switch A

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ Port Config. Configure o modo de funcionamento das portas 11 e 12 como GENERAL e TRUNK respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config. Criar a VLAN com o VLANID 10 nas portas 11 e 12 e configure a regra de saída da porta 11 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ VLAN Config. Criar a VLAN com o VLANID 20 nas portas 11 e 12 e configure a regra de saída da porta 11 como UNTAGGED.
4	Configurar MAC VLAN 10	Obrigatório, VLAN ⟶ MAC VLAN, criar o MAC VLAN 10 com o endereço MAC 00-19-56-8A-4C-71.
5	Configurar MAC VLAN 20	Obrigatório, VLAN ⟶ MAC VLAN, criar o MAC VLAN 10 com o endereço MAC 00-19-56-82-3B-70.

» Configuração do switch B

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Port Config. Configure o modo de funcionamento das portas 21 e 22 como GENERAL e TRUNK respectivamente.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → VLAN Config. Criar a VLAN com o VLANID 10 nas portas 21 e 22 e configure a regra de saída da porta 21 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN → 802.1Q VLAN → VLAN Config. Criar a VLAN com o VLANID 20 nas portas 21 e 22 e configure a regra de saída da porta 21 como UNTAGGED.
4	Configurar MAC VLAN 10	Obrigatório, VLAN → MAC VLAN, criar o MAC VLAN 10 com o endereço MAC 00-19-56-8A-4C-71.
5	Configurar MAC VLAN 20	Obrigatório, VLAN → MAC VLAN, criar o MAC VLAN 10 com o endereço MAC 00-19-56-82-3B-70.

» Configuração do switch C

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN → 802.1Q VLAN → Port Config. Configure o modo de funcionamento das portas 2 e 3 como GENERAL e as portas 4 e 5 como ACCESS.
2	Criar a VLAN 10	Obrigatório, VLAN → 802.1Q VLAN → VLAN Config. Criar a VLAN com o VLANID 10 nas portas 2 e 3 e 5.
3	Criar a VLAN 20	Obrigatório, VLAN → 802.1Q VLAN → VLAN Config. Criar a VLAN com o VLANID 20 nas portas 2 e 3 e 4.

6.6. Exemplos de aplicação de VLAN por Protocolo

» **Requisitos da rede**

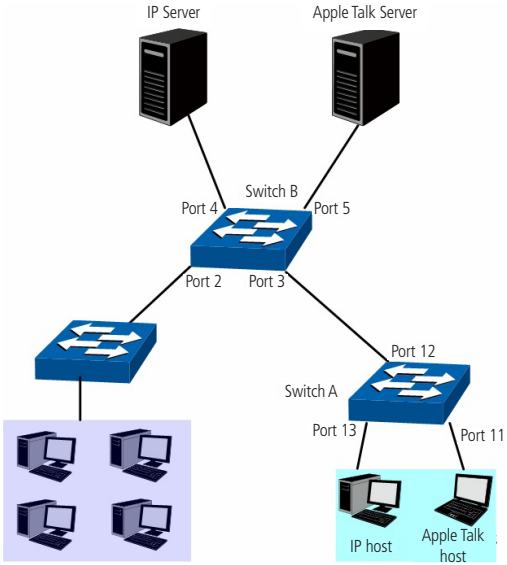
» O departamento A está conectado a rede da empresa pela porta 12 do switch A.

» O departamento A possui computadores que utilizam o protocolo IP e AppleTalk.

» Os computadores que utilizam o protocolo IP são membros da VLAN 10 e utilizam o servidor "IP Server", enquanto os computadores que utilizam AppleTalk são membros da VLAN 20 e utilizam o servidor "AppleTalk server".

» Os servidores "IP server" e "AppleTalk" estão conectados ao switch B.

» **Diagrama da rede**



Aplicação de VLAN por Protocolo

» **Procedimento de configuração**

» Configuração do switch A

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN⟶802.1Q VLAN⟶Port Config. Configure o modo de funcionamento das portas 11 e 13 como ACCESS, e da porta 12 como General.
2	Criar a VLAN 10	Obrigatório, VLAN⟶802.1Q VLAN⟶VLAN Config. Criar a VLAN com o VLANID 10 nas portas 12 e 13 e configure a regra de saída da porta 12 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN⟶802.1Q VLAN⟶VLAN Config. Criar a VLAN com o VLANID 20 nas portas 11 e 12 e configure a regra de saída da porta 12 como UNTAGGED.

» Configuração do switch B

Passo	Operação	Descrição
1	Definir o modo de funcionamento da porta	Obrigatório, VLAN⟶802.1Q VLAN⟶Port Config. Configure o modo de funcionamento das portas 4 e 5 como ACCESS, e da porta 3 como General.
2	Criar a VLAN 10	Obrigatório, VLAN⟶802.1Q VLAN⟶VLAN Config. Criar a VLAN com o VLANID 10 nas portas 3 e 4 e configure a regra de saída da porta 3 como UNTAGGED.
3	Criar a VLAN 20	Obrigatório, VLAN⟶802.1Q VLAN⟶VLAN Config. Criar a VLAN com o VLANID 20 nas portas 3 e 5 e configure a regra de saída da porta 3 como UNTAGGED.
4	Criação do modelo de protocolo	Obrigatório, VLAN → Protocol VLAN → Protocol Template. Criar os Modelos de Protocolos utilizados. Ex: pacotes que utilizam o protocolo de rede IP são encapsulados utilizando o formato Ethernet II e possuem o campo EtherType igual a 0800 já os pacotes que utilizam o protcolo AppleTalk são encapsulados utilizando o formato 802.2 SNAP e possuem o PID (Protocol Identification) igual a 809B. Por padrão estes dois modelos de protocolos já estão definidos.
5	Selecionar as portas participantes da VLAN por Protocolo	Obrigatório, VLAN⟶Protocol VLAN⟶Port Enable. Habilite as portas 3, 4 e 5 para participarem da VLAN por Protocolo.
6	Criar a VLAN por Protocolo 10	Obrigatório, VLAN⟶Protocol VLAN⟶Protocol VLAN. Criar a VLAN por Protocolo com VLANID 10 para o protocolo de rede IP.
7	Criar a VLAN por Protocolo 20	Obrigatório, VLAN⟶Protocol VLAN⟶Protocol VLAN. Criar a VLAN por Protocolo com VLANID 20 para o protocolo de rede Apple Talk.

6.7. GVRP

GVRP (GARP VLAN Registration Protocol) é uma implementação do GARP (Generic Attribute Registration Protocol). GVRP permite que o switch adicione ou remova VLANs automaticamente através de informações dinâmicas de registro de VLANs, propagando as informações de registro da VLAN local para outras sem ter de configurar individualmente cada VLAN.

» **GARP**

GARP fornece mecanismo de auxílio a switches membros de uma LAN a entregar, propagar e registrar as informações de atributos de registros entre os switches. A aplicação que utiliza GARP é chamada de implementação GARP e o GVRP é uma implementação do GARP. Quando o GARP é implementado na porta do switch, a porta é chamada de entidade GARP. A troca de informações entre as entidades GARP é complementada por mensagens. GARP define as mensagens em três tipos: Join, Leave and LeaveAll.

» **Mensagem Join:** uma entidade GARP envia mensagens Join para registrar seus atributos a outras entidades GARP, esta mensagem também pode ser enviada quando a entidade GARP recebe mensagens Join de outras entidades GARP ou quando o registro de seus atributos é configurado manualmente.

» **Mensagem Leave:** uma entidade GARP envia mensagens Leave para remover seus atributos registrados por outras entidades GARP, esta mensagem também pode ser enviada quando a entidade GARP recebe mensagens Leave de outras entidades GARP ou quando os registros de seus atributos são removidos manualmente.

» **Mensagem LeaveAll:** durante a inicialização, a entidade GARP inicia o timer LeaveAll, quando este timer expira é enviada uma mensagem LeaveAll para cancelar todos os seus atributos registrados a todas as entidades GARP participantes.

Através da troca de mensagens, todas as informações de registro dos atributos podem ser propagadas para todos os switches da mesma rede.

- **Hold timer:** quando uma entidade GARP recebe um pedaço de informação de registro, ele não envia imediatamente a mensagem Join. Para economizar recursos de largura de banda ele inicia um temporizador, coloca todas as informações que recebe antes do temporizador acabar e ai sim envia uma mensagem de Join.
- **Join timer:** para transmitir as mensagens Join de forma confiável, a entidade GARP envia duas vezes a mensagem *Join*. O Join Timer é o temporizador usado para definir o intervalo entre o envio das mensagens.
- **Leave timer:** quando uma entidade GARP deseja remover informações de registro de um atributo, ele envia uma mensagem Leave. Quando a entidade GARP recebe essa mensagem, é iniciado um temporizador, caso nenhuma mensagem Join for recebida pela entidade até o temporizador expirar, o registro do atributo será removido da entidade GARP.
- **LeaveAll timer:** durante a inicialização de uma entidade GARP, é iniciado o temporizador LeaveAll, após o término deste temporizador é enviado a mensagem LeaveAll, a fim de informar a todas as outras entidades GARP para que possam voltar a registrar todas as informações do atributo da entidade. Após esta etapa a entidade reinicia o LeaveAll Timer e começa um novo ciclo.
- **GVRP**

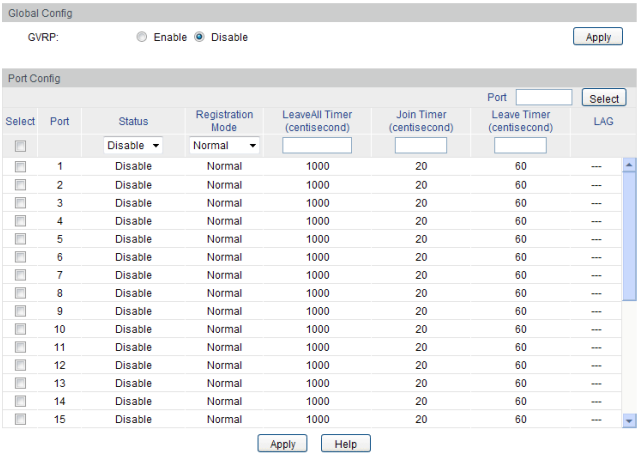
GVRP é uma implementação do GARP. Esta implementação mantém o registro de informações dinâmicas de VLANs e pode também, propagar estas informações para outros switches, adotando o mesmo mecanismo do GARP.

Depois que a função GVRP é habilitada, o switch recebe as informações de registro de VLAN de outros switches para atualizar dinamicamente as informações de registro da VLAN local, incluindo os membros da VLAN e as portas através dos quais os membros de VLANs podem ser alcançados e assim por diante. O switch também propaga as informações de VLAN local para outros switches até que todos os swithes na mesma rede tenham as mesmas informações de VLANs. Informações sobre a inclusão, não inclui somente as informações de registro estático configurado localmente, mas também as informações de registro dinâmico recebido de outros switches.

Neste switch, somente a porta configurada como TRUNK pode ser habilitada para o uso do GVRP. O switch possui os seguintes modos de registro de porta. Normal, Fixed e Forbidden.

- **Normal:** neste modo, a porta pode registrar ou remover dinamicamente uma VLAN além de propagar as informações referente às VLANs dinâmicas e estáticas.
- **Fixed:** neste modo, a porta não pode registrar ou remover dinamicamente uma VLAN, somente propaga informações referente às suas próprias VLANs configuradas manualmente.
- **Forbidden:** neste modo a porta não pode registrar ou remover VLANs, somente propaga informações da VLAN Padrão "VLAN 1".

Escolha o menu *VLAN → GVRP* para acessar a seguinte página:


Global Config
GVRP: Enable Disable
Apply
Port Config
Port
Select
Select Port Status Registration Mode LeaveAll Timer (centisecond) Join Timer (centisecond) Leave Timer (centisecond) LAG
Disable Normal
1 Disable Normal 1000 20 60 ---
2 Disable Normal 1000 20 60 ---
3 Disable Normal 1000 20 60 ---
4 Disable Normal 1000 20 60 ---
5 Disable Normal 1000 20 60 ---
6 Disable Normal 1000 20 60 ---
7 Disable Normal 1000 20 60 ---
8 Disable Normal 1000 20 60 ---
9 Disable Normal 1000 20 60 ---
10 Disable Normal 1000 20 60 ---
11 Disable Normal 1000 20 60 ---
12 Disable Normal 1000 20 60 ---
13 Disable Normal 1000 20 60 ---
14 Disable Normal 1000 20 60 ---
15 Disable Normal 1000 20 60 ---
Apply
Help

Configuração GVRP

Obs.: *se o recurso GVRP está habilitado em uma porta membro de um grupo LAG, por favor, certifique-se que todas as portas membros deste grupo LAG estejam com as mesmas configurações e modos de registro.*

As seguintes informações são exibidas na tela:

» **Global config**

GVRP: selecione *Enable/Disable* para habilitar ou desabilitar a função GVRP no switch e clique em *Apply* para validar a escolha.

» **Port config**

Port select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a função GVRP na porta desejada. O tipo de porta deve estar definido como TRUNK para aceitar o recurso GVRP.

Registration mode: selecione o modo de registro da porta.

» **Normal:** neste modo a porta pode registrar/remover dinamicamente uma VLAN e propagar as informações de VLANs dinâmicas e estáticas.

» **Fixed:** neste modo a porta não pode registrar/remover dinamicamente uma VLAN. Somente propaga as informações de VLANs estáticas.

» **Forbidden:** neste modo a porta não pode registrar/remover VLANs. Somente propaga informações da VLAN 1.

LeaveAll timer: quando o LeaveAll Timer é definido, a porta com GVRP habilitado pode enviar uma mensagem LeaveAll após o timer finalizar, para que outras portas GARP possam registrar as informações de atributos. Depois disso o temporizador LeaveAll vai começar um novo ciclo. O temporizador LeaveAll varia de 1000 a 30000 centésimos de segundo.

Join timer: para garantir a transmissão de mensagens Join, a porta GARP envia a mensagem duas vezes. O Join Timer é usado para definir o intervalo entre o envio das duas mensagens. O Join Timer pode estar na faixa de 20 a 1000 centésimos de segundo.

Leave timer: quando o Leave Timer for definido, a porta GARP recebe uma mensagem de Leave e irá iniciar o seu Leave Timer e removerá os atributos de informação se não receber uma mensagem Join antes do tempo acabar. O Leave Timer está na faixa de 60 a 3000 centésimos de segundos.

LAG: exibe o grupo LAG a qual a porta pertence.

Obs.: *LeaveAll Timer tem que ser >= a 10 vezes o Leave Timer. Já o Leave Timer tem que ser >= a 2 vezes o Join Timer.*

Procedimento de configuração

Passo	Operação	Descrição
1	Configurar o modo de funcionamento da porta	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ Port Config, configurar o modo de funcionamento da porta como Trunk.
2	Habilitar a função GVRP	Obrigatório, VLAN ⟶ GVRP, habilite função GVRP.
3	Configurar o modo de registro e os tempos para porta.	Obrigatório, VLAN ⟶ GVRP, configure os parâmetros da porta baseado nas aplicações atuais.

7. Spanning tree

STP (Spanning Tree Protocol), pertence à norma IEEE802.1d e assegura que haja somente um caminho lógico entre todos os destinos na camada de enlace em uma rede local, fazendo o bloqueio intencional dos caminhos redundantes que poderiam causar um loop. Uma porta é considerada bloqueada quando o tráfego da rede é impedido de entrar ou deixar aquela porta. Isto não inclui os quadros BPDU (Bridge Protocol Data Unit) que são utilizados pelo STP para impedir loops.

BPDU (Bridge Protocol Data Unit) é o quadro de mensagem trocado entre os switches que utilizam a função STP. Cada BPDU contém um campo chamado BID (Bridge ID) que identifica o switch que enviou o BPDU. O BID contém um valor de prioridade, o endereço MAC do switch de envio, e uma ID de Sistema Estendido opcional. Determina-se o valor o BID mais baixo através da combinação destes três campos.

» **Elementos STP**

Bridge ID: indica valor da prioridade e endereço MAC do switch. O switch que possuir o menor Bridge ID terá maior prioridade.

Root bridge: indica o switch que possui o menor Bridge ID. O switch considerado Root Bridge serve como ponto de referência para todos os cálculos STP para garantir melhor desempenho e confiabilidade na rede.

Designated bridge: indica o switch que possui o caminho com menor custo até o Root Bridge em cada segmento de rede. Os quadros BPDUs são encaminhados para o segmento de rede através dos switches Designated Bridge.

Root path cost: indica a soma de todos os custos de porta ao longo do caminho até a Root Bridge. O custo do caminho da Root Bridge é *0*.

Bridge priority: a Bridge Priority pode ser ajustada para um valor no intervalo de 0 a 61440. O valor mais baixo da Bridge Priority possui uma maior prioridade. O switch com a maior prioridade possui maior chance de ser escolhido como Root Bridge.

Root port (porta raiz): indica a porta mais próxima (caminho com menor custo) para a Root Bridge. Por esta porta que os pacotes serão encaminhados para a Root Bridge.

Designated port (porta designada): são todas as Portas Não-Raiz que ainda podem encaminhar tráfego na rede.

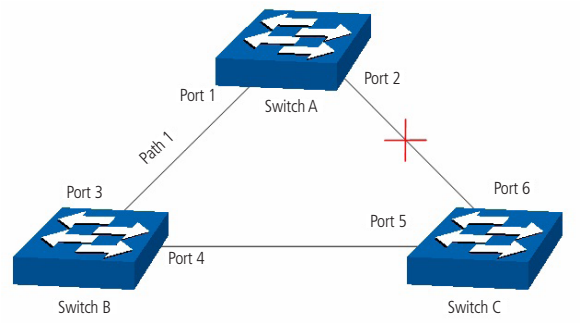
Port priority: a prioridade da porta pode ser ajustada em um intervalo de 0-255. O valor mais baixo para a Port Priority possui maior prioridade. A porta com maior prioridade possui maior chance de ser escolhida como porta raiz.

Path cost: indica o parâmetro para escolha do caminho do link STP. Ao calcular o custo do caminho, o STP escolhe os melhores caminhos entre as ligações redundantes.

O diagrama a seguir mostra o esboço de uma rede Spanning Tree. Os switch A, B e C estão conectados. Após a geração do STP, o switch A é escolhido como Root Bridge, o caminho da porta 2 para porta 6 ficará bloqueado.

» Switches: switch A é o Root Bridge da rede e o switch B é o Designated Bridge do switch C.

» Portas: a porta 3 é a Root Port do switch B e a porta 5 é a Root Port do switch C; a porta 1 é a Designated Port do switch A e a porta 4 é a Designated Port do switch B; a porta 6 do switch C está bloqueada.



Rede spanning tree

» **STP timers**

Hello time: especifica o intervalo de envio de pacotes BPDU. O valor pode variar de 1 à 10 segundos.

Max. age: especifica o tempo máximo que o switch aguarda para remover sua configuração e iniciar uma nova eleição do Root Bridge. O valor pode variar de 6 à 40 segundos.

Forward delay: especifica o tempo para a porta alterar seu estado após uma alteração na topologia da rede. O valor pode variar de 4 à 30 segundos.

Quando a regeneração do STP é causada por um mau funcionamento da rede ou até mesmo uma alteração na topologia da rede, a estrutura do STP começará a realizar as alterações necessárias. No entanto, como os BPDUs da nova configuração não podem ser enviados pela rede de uma só vez, um loop somente ocorreria se o estado da porta estivesse diretamente no estado de encaminhamento. Portanto, o STP adota um mecanismo de estados de portas STP, isto é, a nova Root Port e a Designated Port começam a transmitir dados (estado de encaminhamento) após duas vezes o tempo do Forward Delay, o que garante que os novos BPDUs já tenham sido enviados para toda a rede.

» **Principio de comparação de quadros BPDU**

Supondo dois BPDUs: BPDUx e BPDUy.

Se a ID da Root Bridge do x é menor que a do y, x terá prioridade ao y.

Se a ID da Root Bridge do x é igual a do y, mas o custo do caminho da bridge de x é menor do que a de y, x terá prioridade ao y.

Se a ID da Root Bridge e o custo do caminho de x é igual ao de y, mas o ID da Bridge de x é menor que a de y, x terá prioridade ao y.

Se a ID da Root Bridge, custo do caminho e ID da Bridge de x for igual ao de y, mas a Port ID de x for menor do que a de y, x terá prioridade.

» **Convergência STP**

» **Iniciando**

Ao iniciar, cada switch se considera o Root Bridge e gera uma configuração BPDU para cada porta, com Root Path sendo 0 e o ID da Designated Bridge e Designated Port sendo do próprio switch.

» **Comparando BPDUs**

Cada switch envia BPDUs com suas configurações e recebe BPDUs de outros switches através de suas portas. A tabela a seguir mostra a comparação de operações.

Passo	Operação
1	Se a prioridade da BPDU recebida na porta é menor que a BPDU da própria porta, o switch descarta a BPDU e não altera o BPDU da porta.
2	Se a prioridade da BPDU é maior que a BPDU da porta, o switch substitui o BPDU da porta com a BPDU recebida e compara com a das outras portas no switch para obter a BPDU com maior prioridade.

» **Selecionando o Root Bridge**

O Root Bridge é selecionado pela comparação das BPDUs recebidas. O switch com o Root ID menor é escolhido como Root Bridge.

» **Selecionando a Root Port e a Designate Port**

A operação é realizada da seguinte maneira.

Passo	Operação
1	Para cada switch da rede (exceto o escolhido como Root Bridge), a porta que recebe o BPDU com a prioridade mais alta é escolhida como o Root Port do switch.
2	Utilizando a Root Port BPDU e o Root Path Cost, o switch gera uma Designated Port BPDU para cada uma de suas portas. - Root ID é substituído com o da Root Port. - Root Path é substituído com a soma do Root Path Cost da Root Port e o Path Cost entre a porta e a Root Port. - O ID da Designated Bridge é substituído com o do switch. - O ID da Designated Port é substituído com o da porta.
3	O switch compara o BPDU resultante com o BPDU da porta desejada. - Se o BPDU recebido tem prioridade sobre o BPDU da porta, a porta é escolhida como Designated Port e o BPDU da porta é substituído pelo o BDPU recebido. A porta então envia regularmente o BPDU com maior prioridade. - Se o BPDU da porta tem prioridade sobre o BPDU recebido, o BPDU da porta não será substituído, a porta entra em estado de bloqueio e somente pode receber BPDUs.

Obs.: *o STP em uma rede com topologia estável, somente a Root Port e a Designated Port encaminham dados, as outras portas permanecem no estado de bloqueio. As portas bloqueadas somente podem receber BPDUs.*

O RSTP (IEEE802.1w) é uma evolução do 802.1D padrão. A terminologia de STP do 802.1w permanece essencialmente igual à terminologia de STP do IEEE802.1d. A maioria dos parâmetros permaneceu inalterada, assim os usuários familiarizados com o STP podem configurar rapidamente o novo protocolo.

O RSTP adianta o novo cálculo do spanning tree quando a topologia de rede de Camada 2 é alterada. O RSTP pode obter uma convergência muito mais rápida em uma rede corretamente configurada.

- Condição para a Root Port alterar o estado da porta para "encaminhamento": quando a Root Port do switch deixa de encaminhar dados a Designated Port começa a transmitir dados imediatamente.
- A condição para a Designated Port alterar o estado da porta para "encaminhamento": a Designated Port pode operar de duas formas: edge Port (Porta de Acesso) e Link P2P (conexão direta com outro switch).
  - Se a Designated Port é uma Edge Port: a porta altera imediatamente seus estado para "encaminhamento".
  - Se Designated Port é um Link P2P: a porta somente mudará o estado para "encaminhamento" após realização do handshake entre as portas do switch.
- **Elementos RSTP**

  Edge Port: indica que a porta do switch está conectada diretamente aos terminais.

  P2P Link: indica que a porta do switch está conectada diretamente a outro switch.

MSTP (Multiple Spanning Tree Protocol), referente à norma IEEE802.1s, é compatível tanto com o STP quanto o RSTP, além de permitir a convergência do Spanning Tree, também permite que pacotes de diferentes VLANs sejam transmitidos ao longo de seus respectivos caminhos de modo a proporcionar ligações redundantes com um melhor mecanismo de balanceamento de carga.

Funções do MSTP

- MSTP através das instâncias de VLAN faz com que o switch economize largura de banda durante a convergência e manutenção do STP, interligando várias VLANs a uma instância.
- MSTP divide uma rede com Spanning Tree em várias regiões. Cada região possui sua própria convergência STP que são independentes uma das outras.
- MSTP fornece um mecanismo de equilíbrio de carga para transmissões de pacotes na VLAN.
- MSTP é compatível com STP e RSTP.

Elementos MSTP

Regiões MST (Multiple Spanning Tree Region): uma região MST corresponde aos switches que possuem a mesma configuração de região e Instâncias de VLAN.

IST (Internal Spanning Tree): uma IST é a execução interna do Spanning Tree dentro de uma região MST.

CST (Common Spanning Tree): uma CST é a execução do Spanning Tree em uma rede que conecta todas as regiões MST na rede.

CIST (Common and Internal Spanning Tree): um CIST compreende a IST e CST, é a execução do Spanning Tree que conecta todos os switches da rede.

A figura a seguir exibe o diagrama de uma rede com MSTP:

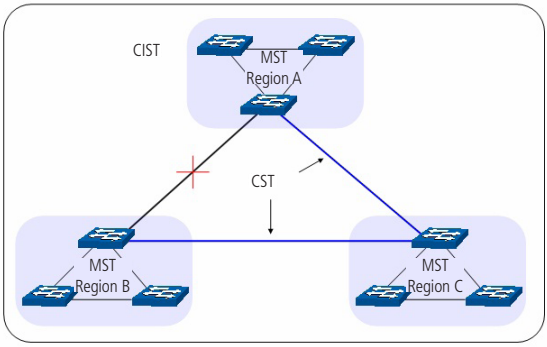


Diagrama de rede MSTP

» **MSTP**

O MSTP divide uma rede em várias regiões. O CST é gerado entre estas regiões do MST, cada região MST pode executar o Spanning Tree. Cada Spanning Tree é chamado de instância. Assim como o STP, o MSTP utiliza BPDUs para a execução do Spanning Tree. A única diferença é que o BPDU do MSTP transporta as informações de configuração MSTP dos switches.

» **Estado das portas**

No MSTP, as portas podem estar nos seguintes estados.

» Forwarding: neste estado a porta pode enviar e receber dados da rede além de enviar e receber quadros BPDUs e aprender endereços MAC.

» Learning: neste estado a porta pode enviar e receber BPDUs e aprender endereços MAC.

» Blocking: neste estado a porta somente receber pacotes BPDUs.

» Disconnected: neste estado a porta não participa da execução do STP.

» **Funções das portas**

Em um MSTP, existem as seguintes funções para as portas.

» Root Port: indica a porta que tem o caminho com menor custo (Path Cost) até o Root Bridge.

» Designated Port: indica a porta que encaminha pacotes para um segmento de rede do switch.

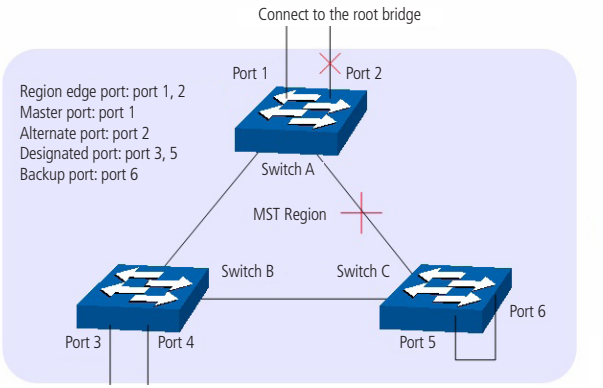
» Master Port: indica a porta que se conecta a região MST de outro switch.

» Alternate Port: indica a porta que pode ser utilizada como backup da Root Port ou Master Port.

» Backup Port: indica a porta de backup da Designated Port.

» Disable: indica a porta que não participa do STP.

O diagrama a seguir exibe as diferentes funções das portas.



Funções das portas em MSTP

A função Spanning Tree possui quatros sub-menus de configuração: *STP Config*, *Port Config*, *MSTP instance* e *STP Security*.

7.1. STP config

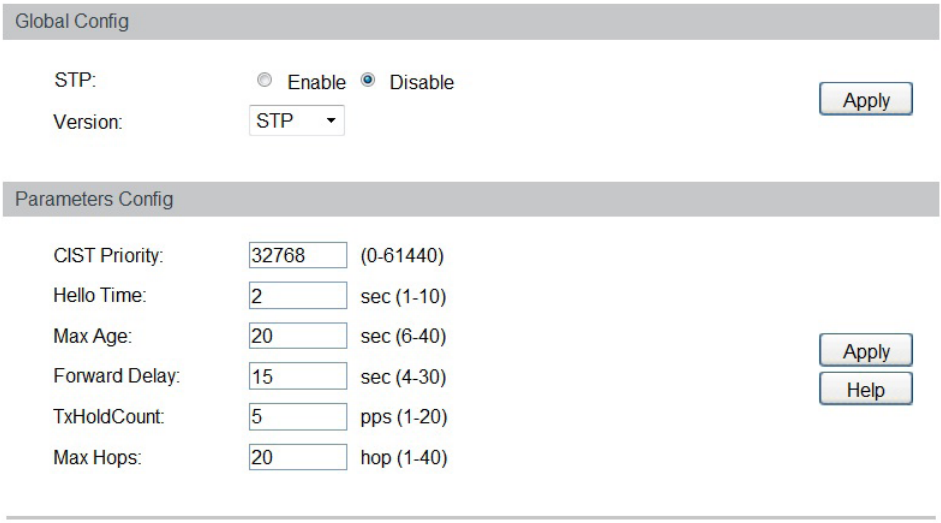
O sub-menu STP Config é utilizado para realizar as configurações globais da função Spanning Tree e podem ser realizados através das páginas: *STP Config* e *STP Summary*.

STP config

Antes de configurar o Spanning Tree em uma rede, é necessário definir a função que cada switch irá desempenhar dentro de uma instância Spanning Tree. Apenas um switch pode ser o Root Bridge em cada instância Spanning Tree.

Nesta página você pode configurar globalmente a função de Spanning Tree e seus parâmetros.

Escolha o menu *Spanning Tree* → *STP Config* → *STP Config* para carregar a seguinte página:



Configuração STP

As seguintes opções são exibidas na tela:

» **Global config**

STP: selecione *Enable/Disable* para habilitar ou desabilitar função STP no switch.

Version: selecione a versão desejada do protocolo STP.

» **STP:** Spanning Tree Protocol.

» **RSTP:** Rapid Spanning Tree Protocol.

» **MSTP:** Multiple Spanning Tree Protocol.

» **Parameters Config**

CIST priority: insira um valor de 0 a 61440 para especificar a prioridade do switch durante a troca de quadros BPDUs. A prioridade CIST é um critério importante na determinação da Root Bridge. O switch com a maior prioridade será escolhido como Root Bridge.

O valor mais baixo tem maior prioridade. O valor padrão é 32768 e deve ser um divisor exato de 4096.

Hello time: insira um valor de 1 a 10 em segundos para especificar o intervalo de envios de quadros BPDUs. A seguinte formula é utilizada para testar o link "2 * (Hello Time + 1) <= Max Age". O valor padrão é 2.

Max age: insira um valor de 6 a 40 em segundos para especificar o tempo máximo que o switch ficará aguardando um quadro BPDU antes de tentar se reconfigurar. O valor padrão é 20 segundos.

Forward delay: insira um valor de 4 a 30 segundos para especificar o tempo para a porta poder alterar seu estado após uma alteração na topologia da rede. A seguinte formula é utilizada "2 * (Forward Delay -1) >= Max Age". O valor padrão é 15 segundos.

TxHoldCount: insira um valor de 1 a 20 para definir o número máximo de pacotes BPDUs transmitidos por intervalo de Hello Time. O valor padrão é 5.

Max hops: insira um valor de 1 a 40 para especificar o máximo de saltos possíveis em uma região específica antes do BPDU ser descartado. O valor padrão é 20 saltos.

Obs.: » *O parâmetro Forward Delay e o diâmetro da rede estão diretamente relacionados. Um pequeno Forward Delay poderá resultar em loops temporários. Um grande Forward Delay poderá resultar na incapacidade da rede voltar ao seu estado normal de operação, durante a convergência STP. O valor padrão é recomendado.*

» *Um Hello Time adequado faz com que o switch possa descobrir as falhas de link ocorridos na rede sem ocupar muito os recursos. Um grande Hello Time, pode resultar em links normais serem detectados como inválidos. Um Hello Time muito pequeno pode resultar em configurações duplicadas sendo enviadas com frequência, o que aumenta a carga nos switches, desperdiçando recursos da rede. O valor padrão é recomendado.*

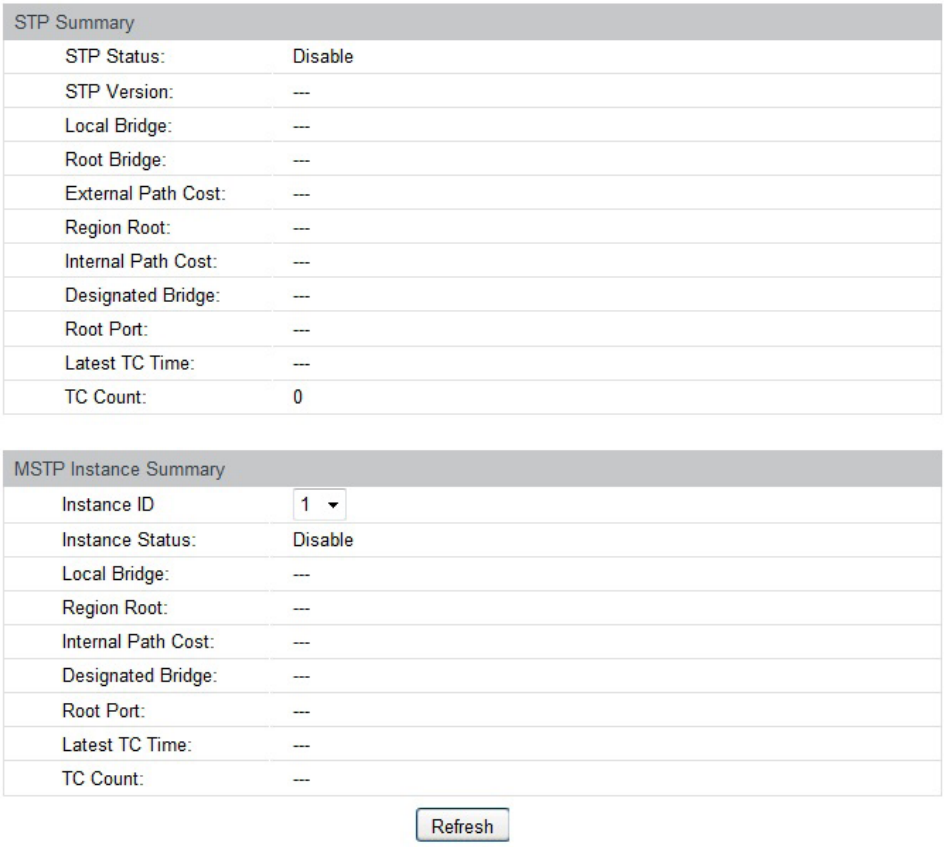
» *Um Max Age pequeno poderá resultar em switches regenerando seus Spanning Tree frequentemente e causando um congestionamento na rede que pode ser confundido como um problema em um dos links. Um Max Age muito grande pode deixar os switches incapazes de encontrar os problemas nos links, causando limitações no Spanning Tree. O valor padrão é recomendado.*

» *Se o parâmetro TxHoldCount for muito alto, o número de pacotes MSTP sendo enviados em cada Hello Time aumentará a utilização da largura de banda da rede. O valor padrão é recomendado.*

STP summary

Nesta página é possível visualizar os parâmetros relacionados à função Spanning Tree.

Escolha no menu *Spanning Tree → STP Config → STP Sumarry* para carregar a seguinte página:

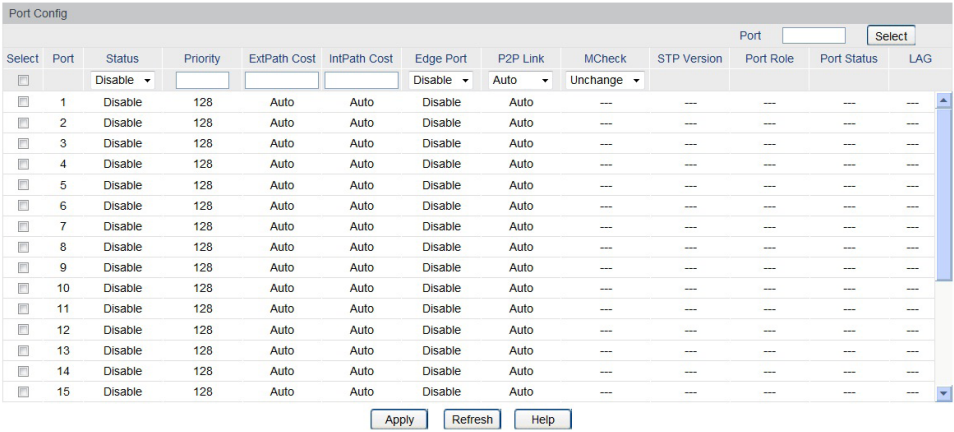


Sumário STP

7.2. Port config

Nesta página é possível configurar os parâmetros das portas STP e de todas as instâncias STP da rede.

Escolha no menu *Spanning Tree → Port Config* para carregar a seguinte página:


Port Config
Port
Select
Select Port Status Priority ExtPath Cost IntPath Cost Edge Port P2P Link MCheck STP Version Port Role Port Status LAG
Disable Disable Auto Unchange
1 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
2 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
3 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
4 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
5 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
6 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
7 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
8 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
9 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
10 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
11 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
12 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
13 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
14 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
15 Disable 128 Auto Auto Disable Auto --- --- --- --- ---
Apply
Refresh
Help
Note:
If the Path Cost of a port is set to 0, it will alter automatically according to the port's link speed.

Portas STP

As seguintes informações são exibidas na tela:

» **Port config**

Port select: digite a porta desejada no campo correspondente e clique em Select para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a função STP na porta desejada.

Priority: digite um valor de 0 a 240 divisível por 16. Port Priority é um importante critério para determinar se a porta conectada será escolhida como Root Port. O valor mais baixo terá maior prioridade.

ExtPath cost: é utilizado para escolher o caminho e calcular os Path Cost das portas em diferentes regiões MST. É um critério importante na definição da Root Port. O valor mais baixo terá maior prioridade.

IntPath cost: é utilizado para escolher o caminho e calcular os Path Cost das portas em uma região MST. É um critério importante na definição da Root Port. O valor mais baixo terá maior prioridade.

Edge port: selecione *Enable/Disable* para habilitar ou desabilitar a função. Esta opção é utilizada conectar um equipamento final (normalmente computadores) na porta do switch. Este modo faz com que o estado da porta se modifique de "Bloqueada" para "Encaminhamento" de forma direta.

P2P link: selecione *Auto/Enable/Disable* para habilitar/desabilitar ou deixar em modo automático o link P2P (portas utilizadas na interconexão de switches). Se as duas portas do link P2P são Root Port ou Designated Port, eles podem alterar o estado da porta para "encaminhamento" de forma mais rápida, reduzindo o tempo de convergência do Spanning Tree.

MCheck: selecione *Enable* para executar a operação Mcheck na porta ou Unchange para não realizar nenhuma operação Mcheck.

STP version: exibe a versão do Spanning Tree da porta.

Port role: exibe a função da porta na instância STP.

» **Root port:** indica a porta que tem o menor Path Cost para a Root Bridge.

» **Designated port:** indica a porta do switch que encaminha pacotes para um segmento de rede.

» **Master port:** indica a porta do switch, que se conecta a região MST de outro switch.

» **Alternate port:** indica a porta que pode ser utilizada como backup da Root Port ou Master Port.

» **Backup port:** indica a porta de backup da Designated Port.

» **Disabled:** indica a porta que não participa do STP.

Port status: exibe o estado de funcionamento da porta.

» **Forwarding (encaminhamento):** neste estado a porta pode receber e enviar dados, receber e enviar quadros BPDUs bem como aprender endereços MAC.

» **Learning (aprendizado):** neste estado a porta pode receber e enviar quadros BPDUs e aprender o endereço MAC.

» **Blocking (bloqueado):** neste estado a porta somente pode receber quadros BPDUs.

» **Disconnected (desconectado):** neste estado a porta não participa do Spanning Tree.

LAG: exibe o número do grupo Lag que a porta pertence.

Obs.: » *Configurar as portas que estão conectadas diretamente aos equipamentos finais (como por exemplo, computadores) como Edge Port e habilitar a função de proteção BPDU. Além de alterar o estado da porta para "encaminhamento" de forma mais rápida, aumenta também a segurança na rede.*

» *Todas as portas pertencentes a grupos LAGs podem ser configuradas como links ponto-a-ponto (P2P Link).*

» *Quando um link de uma porta é configurado como ponto-a-ponto, as instâncias de Spanning Tree possuem suas portas configuradas como ponto-a-ponto (P2P Link). Se a conexão física da porta não for um link ponto-a-ponto, poderá ocorrer loops temporários na rede.*

7.3. MSTP instance

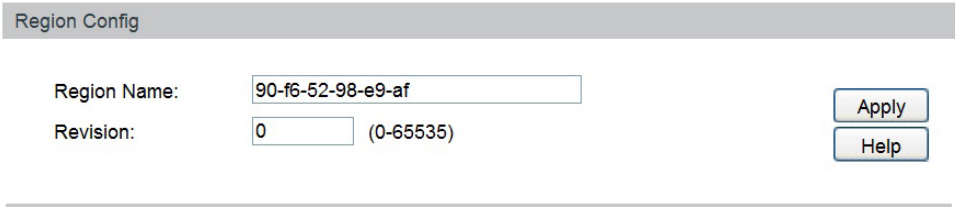
O MSTP cria uma tabela de mapeamento entre VLANs e o Spanning Tree. Ao adicionar uma instância MSTP, várias VLANs são conectadas a uma instância MSTP. Somente os switches que possuem o mesmo nome, revisão e tabela de mapeamento pertencem a mesma região MST.

A função de instância MSTP pode ser configurada nas páginas: *Region Config*, *Instance Config* e *Instance Port Config*.

Region config

Nesta página você pode configurar o nome e revisão da região MST.

Escolha o menu *Spanning Tree → MSTP Instance → Region Config* para carregar a seguinte página:



Região MST

As seguintes opções são exibidas na tela:

» **Region config**

Region name: insira um nome para identificar a região MST, utilizando no máximo 32 caracteres.

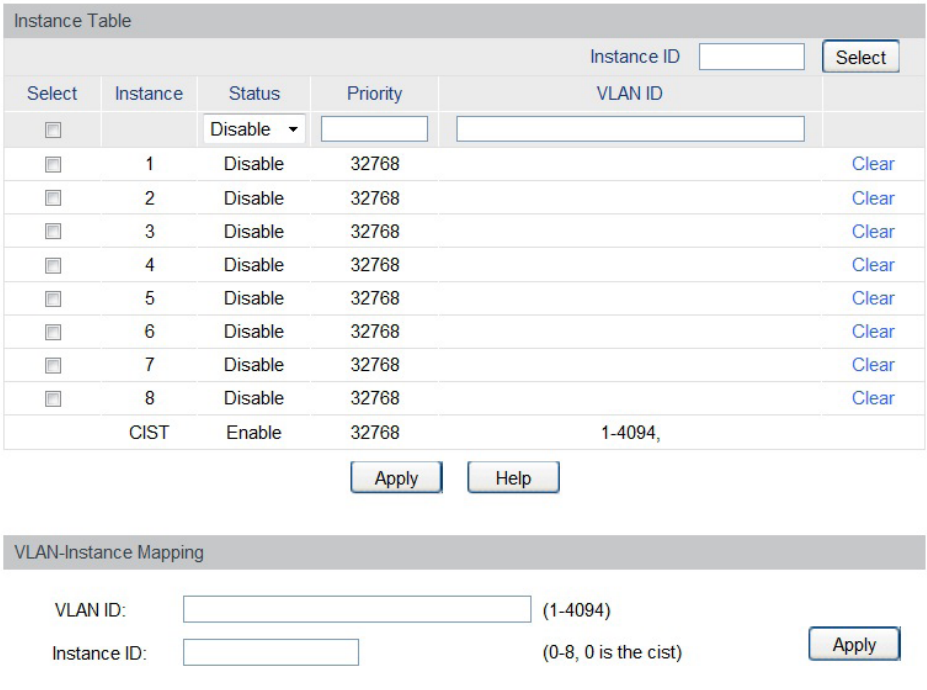
Revision: insira um valor de revisão de 0 a 65535 para identificar a região MST.

Instance config

Nesta página é possível configurar as instâncias MSTP, uma propriedade da região MST, é usado para descrever a VLAN e configuração de mapeamento de instância. Você pode atribuir VLANs a diferentes instâncias de acordo com suas necessidades.

Cada Instância é um grupo de VLANs independente uma das outras e do CIST.

Escolha no menu *Spanning Tree → MSTP Instance → Intance Config* para carregar a seguinte página:



Instâncias MSTP

As seguintes informações são apresentadas na tela:

» **Instance table**

Instance ID select: digite a ID da instância desejada no campo correspondente e clique em *Select* para selecioná-la.

Select: selecione a Instância desejada. Nesta opção é possível selecionar mais de uma Instância simultaneamente.

Instance: exibe o ID da instância MSTP.

Status: selecione *Enable/Disable* para habilitar ou desabilitar o funcionamento da Instância desejada.

Priority: digite a prioridade da instância. É um critério importante para determinar se o switch será escolhido como Root Bridge na instância selecionada.

VLAN ID: digite o VLAN ID que pertence ao ID da instância correspondente. Após a modificação, a VLAN ID será apagada e mapeada para a CIST.

Clear: clique no botão *Clear* para apagar todas as VLANs ID da instância desejada.

» **VLAN-instance mapping**

VLAN ID: digite a VLAN ID desejada, após a modificação, a nova VLAN ID será adicionada a identificação da instância correspondente e a VLAN ID anterior será substituída.

Instance ID: digite o ID da instância correspondente.

Obs.: *em uma rede com GVRP e MSTP habilitados, pacotes GVRP são encaminhados ao longo da CIST. Se você quiser transmitir pacotes de uma VLAN específica através do GVRP, por favor, certifique-se de mapear a VLAN para CIST durante a configuração da tabela de encaminhamento de VLAN.*

Instance port config

Uma porta pode desempenhar diferentes papéis na instância Spanning Tree. Nesta página você pode configurar os parâmetros das portas em ID's de instâncias diferentes, bem como visualizar o status das portas.

Escolha o menu *Spanning Tree → MSTP Instance → Instance Port Config* para carregar a seguinte página:

Port Config
Instance ID
1
Port
Select
Select
Port
Priority
Path Cost
Port Role
Port Status
LAG
1 128 Auto --- --- ---
2 128 Auto --- --- ---
3 128 Auto --- --- ---
4 128 Auto --- --- ---
5 128 Auto --- --- ---
6 128 Auto --- --- ---
7 128 Auto --- --- ---
8 128 Auto --- --- ---
9 128 Auto --- --- ---
10 128 Auto --- --- ---
11 128 Auto --- --- ---
12 128 Auto --- --- ---
13 128 Auto --- --- ---
14 128 Auto --- --- ---
15 128 Auto --- --- ---
Apply
Refresh
Help
Note:
If the Path Cost of a port is set to 0, it will alter automatically according to the port's link speed.

Configuração das instâncias MSTP

As seguintes opções são exibidas na tela:

» **Port config**

Instance ID: selecione o ID da instância desejada para configurar os parâmetros da porta.

Port select: digite a porta deseja no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Priority: digite a prioridade da porta na instância. É um critério importante ao determinar se a porta conectada será escolhida como Root Port.

Path cost: digite o valor utilizado para determinar o custo do caminho da porta em uma região MST. É um critério importante na determinação da Root Bridge. O valor mais baixo terá maior prioridade.

Port role: exibe a função da porta em uma instância MSTP.

Port status: exibe o status de funcionamento da porta.

LAG: apresenta o número do grupo LAG a qual a porta pertence.

Obs.: *o Port Status de uma mesma porta pode ser diferente em instâncias MSTP distintas.*

Configuração global da função Spanning Tree

Passo	Operação	Descrição
1	Deixar claro os papéis de cada switch nas instâncias de STP: Root Bridge ou Designated Bridge.	Preparação
2	Configuração dos parâmetros globais de MSTP.	Obrigatório. Habilitar o STP no switch e configurar os parâmetros MSTP em: Spanning Tree ⟶ STP Config ⟶ STP Config
3	Configuração dos parâmetros MSTP por porta.	Obrigatório, Configurar os parâmetros MSTP para cada porta: Spanning Tree->Port Config-> Port Config
4	Configuração da região MST	Obrigatório, Criar a região MST e configurar a função que o switch desempenhará na região MST em: Spanning Tree ⟶ MSTP Instance ⟶ Region Config e Instance Config.
5	Configuração dos parâmetros das portas para cada Instância MSTP.	Opcional, Configurar diferentes instâncias na região MST e configurar os parâmetros das portas para cada instância MSTP: Spanning Tree ⟶ MSTP Instance ⟶ Instance Port.

7.4. STP security

Neste sub-menu é possível configurar a função de proteção STP, pode-se proteger o switch contra dispositivos maliciosos que tentem realizar ataque contra recursos STP. A função STP Security é configurada nas seguintes páginas: *Port Protect* e *TC Protect*.

Port Protect evita que dispositivos maliciosos ataquem recursos do STP.

Port protect

Nesta página você pode configurar o recurso de proteção de loop, proteção de root, proteção TC, proteção de BPDU e filtro de BPDU por portas.

» **Loop protect**

Em uma rede estável, o switch mantém o estado das portas recebendo e processando quadros BPDU. No entanto, quando ocorre congestionamento no link, falhas na conexão ou alteração indevida na topologia da rede, o switch pode não receber quadros BPDU por um determinado período, resultando em uma nova execução do algoritmo Spanning Tree, podendo ocorrer a alteração do estado das portas antes da convergência STP da rede, isto é, as portas passariam do estado bloqueado (Blocked) para o estado de encaminhamento (Forwarding) precocemente, podendo ocasionar loops na rede.

» **Root protect**

Um CIST e suas Root Bridges secundárias estão geralmente localizados no core da rede. Configurações erradas ou ataques maliciosos podem resultar com que quadros BPDUs com maior prioridades sejam recebidas pelo Root Bridge, o que faz com que Root Bridge atual perca a sua posição, podendo ocasionar atrasos na rede.

Para evitar isso, o MSTP fornece a função Root Protect. As portas que estiverem com esta função habilitada só podem ser definidas como Designateds Ports em todas as instâncias do Spanning Tree. Quando este recurso está habilitado na porta e esta porta receber quadros BPDU com maior prioridade, a porta transitará seu estado para bloqueado "Blocked" negando o encaminhamento de pacotes (como se o link estivesse desconectado). A porta retorna seu estado normal se não receber quadros de configuração BPDUs com prioridades maiores em um período igual a duas vezes o tempo do Forward Delay.

» **TC protect**

O switch remove as entradas de endereços MAC ao receber pacotes TC-BPDU. Se um usuário mal intencionado envia uma grande quantidade de pacotes TC-BPDU para um switch em um curto intervalo de tempo, o switch ficará ocupado realizando a remoção das entradas de endereços MAC, ocasionando a diminuição do desempenho e estabilidade da rede.

Para evitar que o switch remova endereços MAC com frequência, você pode habilitar a função TC Protect. Com o TC Protect habilitado, será possível determinar a quantidade de pacotes TC-BPDU que a porta poderá receber, definindo um número máximo de recebimento de pacotes no campo TC Threshold, desta forma, o switch não executará a operação de remoção dos endereços MAC, impedindo que o switch fique removendo com frequência as entradas de endereços MAC.

» **BPDU protect**

As portas do switch conectadas diretamente em computadores ou servidores podem ser configuradas como Edge Port, para que o estado da porta seja alterado rapidamente, otimizando o processo de convergência STP. As portas configuradas como Edge Port não podem receber quadros BPDUs. Quando essas portas recebem BPDUs, o sistema automaticamente configura essas portas como Non-Edge e regenera o Spanning Tree, podendo causar atrasos na convergência do STP. Um usuário mal intencionado pode atacar o switch enviando quadros BPDUs, que resultaria em atrasos na convergência do STP.

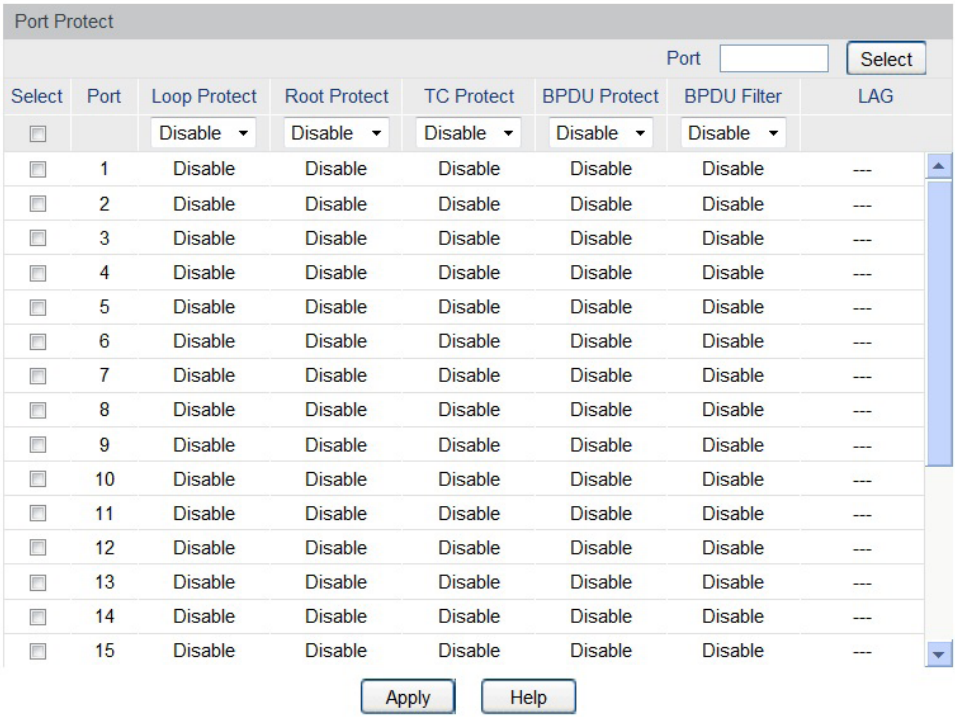
Para evitar esse tipo de ataque, o MSTP fornece a função de BPDU Protect. Com essa função habilitada, o switch desabilita as portas configuradas como Edge Port ao receberem quadros BPDUs e relata esses casos ao administrador. Se uma porta for desabilitada, somente o administrador poderá restaurá-la.

» **BPDU filter**

Esta proteção é utilizada para evitar uma inundação de BPDUs na rede STP. Se um switch recebe BPDUs maliciosos, ele encaminha estas BPDUs para outros switches conectados na rede, podendo fazer com que o Spanning Tree seja constantemente regenerado. Neste caso o processador do switch ficará sobrecarregado além destas BPDUs atrapalharem a convergência STP.

Com a função BPDU Filter habilitada, uma porta não pode receber ou transmitir BPDUs, apenas envia seus próprios BPDUs. Tal mecanismo evita que o switch seja atacado por BPDUs maliciosas, Garantido que a convergência STP esteja correta.

Entre no menu *Spanning Tree → STP Security → Port Protect* para carregar a seguinte página:



Port protect

As seguintes opções são apresentadas a tela:

» **Port protect**

Port select: digite a porta deseja no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Loop protect: selecione *Enable/Disable* para habilitar ou desabilitar a função Loop Protect na porta desejada. Esta função evita loops na rede, ocasionada por falhas nos links ou congestionamento na rede.

Root protect: selecione *Enable/Disable* para habilitar ou desabilitar a função Root Protect na porta desejada. Esta função evita a alteração da topologia da rede de forma errada, causada pela alteração da Root Bridge atual.

TC protect: selecione *Enable/Disable* para habilitar ou desabilitar a função TC Protect na porta desejada. Esta função previne a diminuição do desempenho e estabilidade do switch ao receber um número grande de pacotes TC-BPDUs.

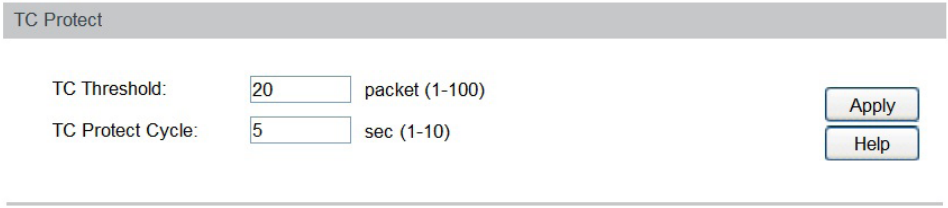
BPDU protect: selecione *Enable/Disable* para habilitar ou desabilitar a função BPDU Protect na porta desejada. Esta função previne que a Edge Port seja atacada por BPDUs maliciosas.

LAG: exibe o número do grupo LAG a qual a porta pertence.

TC protect

Quando a porta do switch está com a função TC Protect habilitada, será necessário configurar a quantidade de pacotes TC-BPDUs e o intervalo de tempo de monitoramento utilizado pela função. Estes parâmetros são configurados na página de configuração TC Protect.

Entre no menu *Spanning Tree* → *STP Security* → *TC Protect* para carregar a seguinte página:



TC protect

As seguintes opções são exibidas na tela:

» **TC protect**

TC threshold: digite o número máximo de pacotes TC-BPDUs que podem ser recebidos em um ciclo TC Protect. A quantidade varia de 1 a 100, o valor padrão é 20.

TC protect cycle: digite o tempo de duração de um ciclo TC Protect. O tempo varia de 1 a 10 segundos, o valor padrão é 5 segundos.

7.5. Exemplos de aplicações para STP

» **Requisitos de rede.**

» Switch A, B, C, D e E todos com suporte a MSTP.

» Switch A, será o switch central.

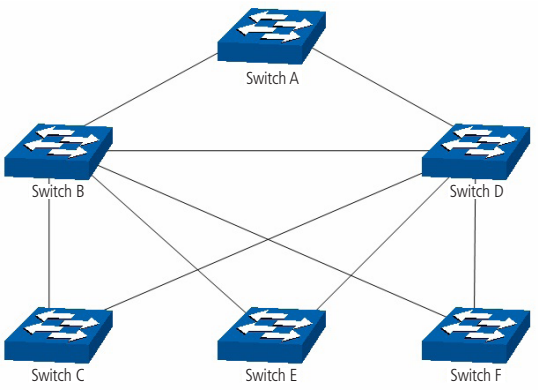
» B e C são switches de convergência. D, E e F são switches da camada de acesso.

» Existem 6 VLANs, rotuladas como VLAN101 a VLAN106 na rede.

» Todos os switches executam o MSTP pertencem à mesma região MSTP.

» Os dados da VLAN101, 103 e 105 são transmitidos pelo STP com o switch B sendo o Root Bridge. Os dados da VLAN102, 104 e 106 são transmitidos pelo STP com o switch C sendo o Root Bridge.

» **Diagrama de rede**



Exemplo de aplicação para STP

» **Procedimento de configuração**

» Configuração do switch A:

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como TRUNK, e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q VLAN.
2	Habilitar a função STP	Spanning Tree⟶STP Config⟶STP Config, habilite a função STP e selecione a versão MSTP. Spanning Tree⟶STP Config⟶Port Config, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree⟶MSTP Instance⟶Region Config, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância 1 e mapeie a VLAN 102. 104 e 106 para instância 2.

» Configuração do switch B

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como TRUNK, e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q
2	Habilitar a função STP	Spanning Tree⟶STP Config⟶STP Config, habilite a função STP e selecione a versão MSTP. Spanning Tree⟶STP Config⟶Port Config, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree⟶MSTP Instance⟶Region Config, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância e mapeie a VLAN 102. 104 e 106 para instância 2.
5	Configure o switch B como root bridge para instância 1	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a prioridade da instância 1 para 0.
6	Configuração das Designated Bridge da instância 2.	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a prioridade da instância 2 para 4096.

» Configuração do switch C:

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como TRUNK, e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q VLAN.
2	Habilitar a função STP	Spanning Tree⟶STP Config⟶STP Config, habilite a função STP e selecione a versão MSTP. Spanning Tree⟶STP Config⟶Port Config habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree⟶MSTP Instance⟶Region Config, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância 1e mapeie a VLAN 102. 104 e 106 para instância 2.
5	Configure o switch C como Root Bridge para instância 1	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a prioridade da instância 1 para 0.
6	Configure o switch C como Designated Bridge para a instância 2.	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a prioridade da instância 2 para 4096.

» Configuração do switch D

Passo	Operação	Descrição
1	Configuração do modo de funcionamento das portas	VLAN ⟶ 802.1Q VLAN, configure o modo de funcionamento das portas como TRUNK, e adicione nas portas correspondentes as VLAN 101 e VLAN 106. As instruções detalhadas podem ser encontradas na seção 802.1Q VLAN.
2	Habilitar a função STP	Spanning Tree⟶STP Config⟶STP Config, habilite a função STP e selecione a versão MSTP. Spanning Tree⟶STP Config⟶Port Config, habilite a função MSTP para as portas.
3	Configuração do nome e revisão da região MST	Spanning Tree⟶MSTP Instance⟶Region Config, configure a região como INTELBRAS e mantenha a configuração de revisão padrão.
4	Configuração da Tabela de Encaminhamento da região MST	Spanning Tree⟶MSTP Instance⟶Instance Config, configure a tabela de encaminhamento. Adicione a VLAN 101, 103 e 105 para a instância 1e mapeie a VLAN 102. 104 e 106 para instância 2.

» O procedimento de configuração dos switches E e F são as mesmas do switch D.

» **Diagrama da topologia das duas instâncias, após a convergência STP**

» Para a instância 1 (VLAN 101,103 e 105), os caminhos em vermelhos na figura a seguir são os links ativos, os caminhos cinza são os links bloqueados.

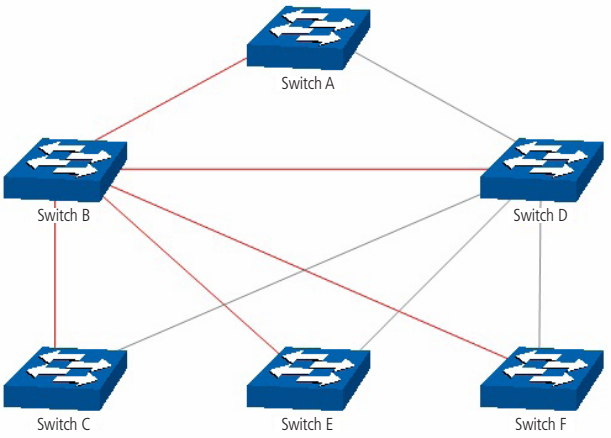


Diagrama da Instância 1 após a convergência STP

» Para a instância 2 (VLAN 102, 104 e 106) os caminhos em azul na figura a seguir são os links ativos, os caminhos cinza são os links bloqueados.

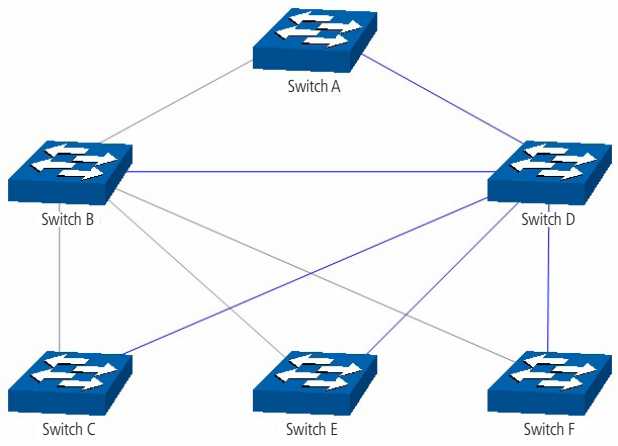


Diagrama da Instância 2 após a convergência STP

» **Sugestões para configuração**

» Habilitar o TC Protect para todas as portas dos switches.

» Habilitar o Root Protect em todas as portas do switch Root Bridges.

» Habilitar o Loop Protect nas portas Non-Edge.

Habilitar a BPDU Protect ou BPDU Filter para as portas que estão conectadas diretamente em computadores ou servidores.

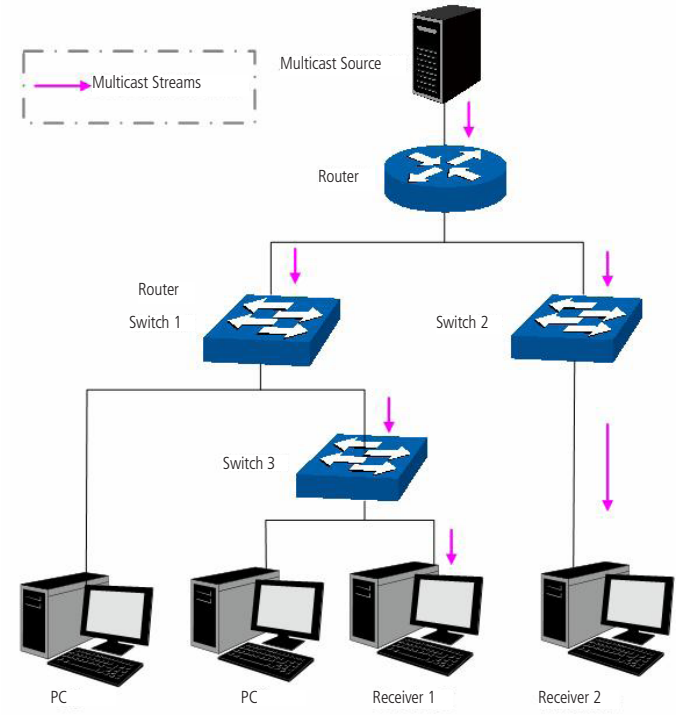
8. Multicast

» **Visão global do Multicast**

Multicast é o método de transmissão de um pacote de dados a múltiplos destinos ao mesmo tempo. O servidor Multicast envia os pacotes de dados somente uma vez, ficando a cargo dos clientes captarem esta transmissão e reproduzi-la, esta técnica diminui consideravelmente o tráfego da rede e é utilizado principalmente em aplicações de streaming de áudio e vídeo conferência. Este método possui uma alta eficiência na entrega dos pacotes a múltiplos clientes, reduzindo a carga da rede.

Este switch utiliza o protocolo IGMP (Internet Group Management Protocol) para consultar quais clientes desejam receber o serviço Multicast ofertado. Com a utilização deste procolo o switch consegue identificar em qual porta o cliente está conectado para receber a transmissão Multicast, a partir desta identificação, o switch encaminha o tráfego Multicast apenas para as portas onde houver solicitante.

A figura a seguir mostra como o tráfego Multicast é transmitido.



Tráfego Multicast

Funções do Multicast

1. Em uma rede ponto-a-multiponto, o número de clientes solicitando um serviço é desconhecido, neste caso, o Multicast otimiza os recursos da rede.
2. Os clientes que recebem a mesma informação do servidor Multicast, formam um Grupo Multicast, Deste modo o servidor Multicast necessita enviar apenas uma única vez a mensagem.
3. Cada cliente pode entrar ou sair do Grupo Multicast a qualquer momento.
4. Em aplicações em tempo real, é aceitável ocorrer algumas perdas de pacotes (dentro de um limite que não prejudique o serviço).

» **Endereços Multicast**

1. Endereços IP Multicast:

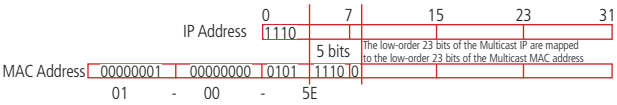
Conforme especificado pelo IANA (Internet Assigned Numbers Authority), os endereços Ips de classe D são usados como endereços Multicast. O intervalo de endereços Multicast vai de 224.0.0.0 a 239.255.255.255. A tabela a seguir exibe o intervalo e descrição de vários endereços Multicast especiais.

Faixa de endereços Multicast	Descrição
224.0.0.0 ~ 224.0.0.255	Endereços Multicast reservados para protocolos de roteamento e outros protocolos de rede.
224.0.1.0 ~ 224.0.1.255	Endereços para videoconferência
239.0.0.0 ~ 239.255.255.255	Endereços Multicast utilizados no gerenciamento da rede local

2. Endereços MAC de Multicast

Quando um pacote Unicast é transmitido em uma rede Ethernet, o endereço MAC de destino é o endereço MAC do receptor. Quando um pacote Multicast é transmitido em uma rede Ethernet, o destino não é apenas um receptor, mas um grupo com um número indeterminado de membros. Para um determinado endereço MAC Multicast, é criado um endereço MAC lógico, utilizado como endereços de destino do pacote.

Conforme estipulado pela IANA, os 24 bits de maior ordem de um endereço MAC Multicast inicia-se com "01-00-5E" enquanto os 23 bits de menor ordem do endereço IP Multicast substituem os 23 bits de menor ordem do endereço MAC, formando assim o endereço MAC Multicast, como mostra a figura a seguir:



Endereço MAC Multicast

» **Tabela de endereços Multicast**

O switch encaminha pacotes Multicast com base na Tabela de endereços Multicast. Como a transmissão de pacotes Multicast não pode se estender a VLANs, a primeira parte da Tabela de endereços Multicast é o VLAN ID, a partir do qual, os pacotes Multicast recebidos são transmitidos somente na VLAN que a porta pertence.

A Tabela de endereços Multicast não está mapeada para uma porta de saída, mas sim, para uma lista de portas pertencentes a um grupo. Ao encaminhar um pacote Multicast, o switch verifica sua Tabela de endereços Multicast, baseado no endereço de destino do pacote Multicast. Se a entrada correspondente não for encontrada na tabela, o switch irá transmitir via broadcast o pacote na VLAN. Se a entrada correspondente for encontrada na tabela, isso indica que o endereço MAC de destino deve estar na lista de grupos de portas, de modo que o switch irá duplicar estes dados de destino e entregará uma cópia para cada porta. O formato geral da tabela de endereços Multicast é descrito na figura a seguir:

VLAN ID	Multicast IP	Port

Tabela de endereços Multicast

» **IGMP snooping**

O IGMP Snooping é um mecanismo de controle Multicast, que pode ser usado no switch para registrar dinamicamente um grupo Multicast. O switch executando o IGMP snooping, gerencia e controla o grupo Multicast escutando e processando mensagens IGMP transmitidas entre os clientes e servidores Multicast, determinando os dispositivos conectados a ele e que pertencem ao mesmo grupo, evitando desta forma que os grupos Multicast transmitam pacotes via broadcast na rede.

A função Multicast possui quatro sub-menus de configuração: *IGMP Snooping, Multicast IP, Multicast Filter* e *Packet Statistic*.

8.1. IGMP snooping

» **Processo IGMP snooping**

O switch executando IGMP Snooping fica escutando as mensagens transmitidas entre os clientes e o servidor Multicast, controlando e registrando as mensagens IGMP que passam por suas portas. Ao receber mensagens IGMP Report, o switch adiciona a porta na Tabela de endereços MAC Multicast, quando o switch escuta mensagens IGMP Leave a partir de um cliente, ele aguarda o servidor Multicast enviar mensagens IGMP Query ao Grupo Multicast especifico para verificar se os outros clientes do grupo ainda necessitam das mensagens Multicast: se sim, o servidor Multicast receberá mensagem IGMP Report, se não, o servidor Multicast não receberá mensagens IGMP Report, portanto o switch removerá a porta específica da Tabela de endereços Multicast.

O servidor Multicast envia regularmente mensagens IGMP Query, após o envio destas mensagens, o switch irá remover a porta da Tabela de endereços Multicast, caso não escute nenhuma mensagem IGMP Report do cliente em um determinado período de tempo.

» **Mensagens IGMP**

O switch, executando IGMP Snooping, processa as mensagens IGMP das seguintes formas:

1. IGMP Query (Consulta IGMP)

   As mensagens IGMP Query (Consulta IGMP) enviadas pelo servidor Multicast podem ser classificadas de duas formas: IGMP General Query (Consulta Geral) ou Group-Specific-Query (Consulta a Grupo Específico). O servidor envia regularmente mensagens de consulta geral, para verificar se os grupos Multicast possuem membros. Ao receber mensagens IGMP Leave, o switch encaminhará as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast.

2. IGMP Report (Relatório IGMP)

   As mensagens IGMP Report são enviadas pelos clientes quando ele deseja se associar (join) a um grupo Multicast ou responder as mensagens de consulta IGMP (IGMP Query) do servidor Multicast.

   Ao receber uma mensagem IGMP Report, o switch encaminhará a mensagem de relatório através da porta denominada "Router Port" para o servidor Multicast, além de analisar a mensagem para obter o endereço do grupo Multicast que o cliente irá se juntar.

   A porta de recepção do switch procederá da seguinte maneira: se a porta que o cliente está conectado no switch é um novo membro para um grupo Multicast, a porta será adicionada a Tabela de endereços Multicast, se a porta que o cliente está conectado já pertence ao grupo Multicast, o tempo de permanência da porta ao grupo Multicast será reiniciado.

3. IGMP Leave (Remoção do Grupo Multicast)

   Clientes que executam o IGMP v1 não enviam mensagens IGMP Leave ao sair de um grupo Multicast, como resultado, o switch somente removerá a porta da Tabela de endereços Multicast após o término do tempo de vida da porta na tabela de endereços. Os clientes que executam IGMP v2 ou IGMP v3, enviam mensagens IGMP Leave ao sair de um grupo Multicast para informar ao servidor Multicast a sua saída.

   Ao receber mensagens IGMP Leave, o switch encaminha as mensagens de consulta ao grupo Multicast específico enviadas pelo servidor Multicast para as portas pertencentes ao grupo, para verificar se outros membros do grupo ainda necessitam do serviço Multicast e reiniciar o tempo de permanência da porta na Tabela de endereços Multicast.

» **Fundamentos do IGMP snooping**

1. Portas

   Router port: indica a porta do switch conectada diretamente ao servidor Multicast.

   Member port: indica a porta do switch conectado diretamente a um membro (cliente) do grupo Multicast.

2. Temporizadores

   Router port time: se o switch não receber mensagens IGMP Query da porta em que o servidor Multicast está conectado dentro de um intervalo de tempo, a porta não será mais considerada como Router Port. O valor padrão é 300 segundos.

   Member port time: se o switch não receber mensagens IGMP Report da porta em que os membros (cliente) de um grupo Multicast estão conectados dentro de um intervalo de tempo, a porta não será mais considerada como Member Port. O valor padrão é 260 segundos.

   Leave time: indica o intervalo entre o switch receber uma mensagem Leave a partir de um cliente e o servidor Multicast remover o cliente do grupo Multicast. O valor padrão é 1 segundo.

A função IGMP Snooping pode ser configurada nas seguintes páginas: *Snooping Config, Port Config, Vlan Config* e *Multicast VLAN*.

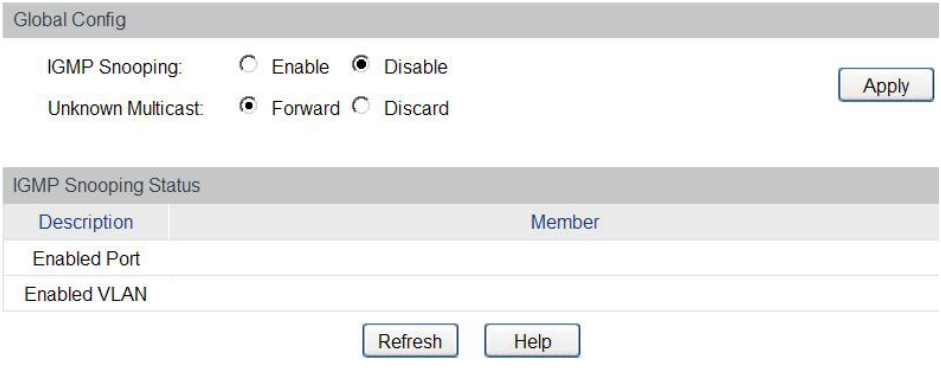
Snooping config

Nesta página é possível habilitar a função IGMP Snooping no switch.

Se o endereço Multicast dos dados recebidos não estiver na tabela de endereços Multicast, o switch irá enviar um broadcast na VLAN.

Quando a função Multicast desconhecido está selecionada em *Discard*, o switch descartará os pacotes de Multicast desconhecidos que são recebidos, evitando assim o uso desnecessário de largura de banda e melhorando a performance do sistema. Por favor, configure esse recurso de acordo com suas necessidades.

Escolha o menu *Multicast* → *IGMP Snooping* → *Snooping Config* para carregar a seguinte página.



Configuração IGMP snooping

» **Global config**

IGMP snooping: selecione *Enable/Disable* para habilitar ou desabilitar a função IGMP Snooping no switch.

Unknown multicast: selecione a operação que o switch irá fazer ao receber Multicast desconhecido:

Forward: o switch encaminhará o pacote Multicast em forma de broadcast à todas as portas pertencentes à VLAN.

Discard: o switch descartará os pacotes Multicast desconhecido que são recebidos, evitando assim o uso desnecessário de largura de banda e melhorando a performance do sistema.

» **IGMP snooping status**

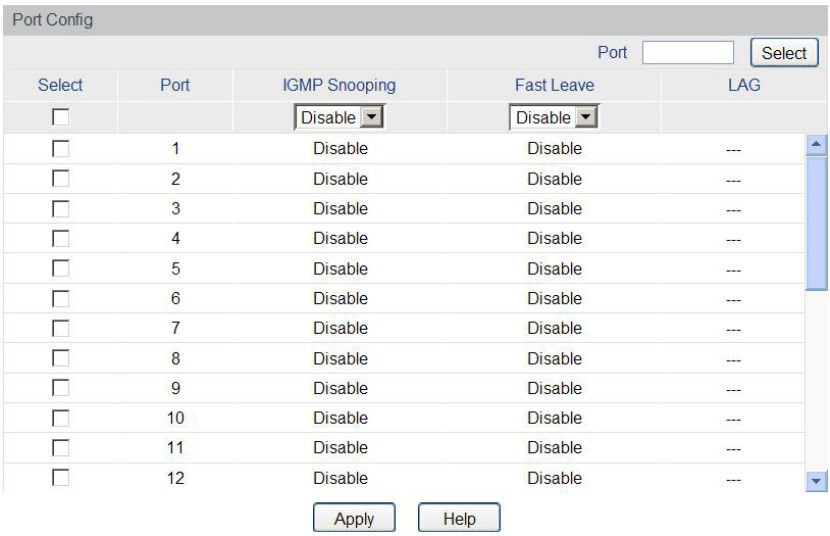
Description: exibe o status da configuração IGMP Snooping.

Member: exibe as portas e VLANs habilitadas para a função IGMP Snooping.

Port config

Nesta página você pode configurar a função IGMP nas portas desejadas do switch.

Entre no menu *Multicast* → *IGMP Snooping* → *Port Config* para carregar a seguinte página:



Port config

As seguintes opções são exibidas na tela:

» **Port config**

Port select: digite a porta deseja no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

IGMP snooping: selecione *Enable/Disable* para habilitar ou desabilitar a função IGMP Snooping na porta desejada.

Fast leave: selecione *Enable/Disable* para habilitar ou desabilitar a função Fast Leave na porta desejada. A função Fast Leave faz com o switch remova imediatamente a porta da Tabela de endereços Multicast, assim que receber uma mensagem IGMP Leave.

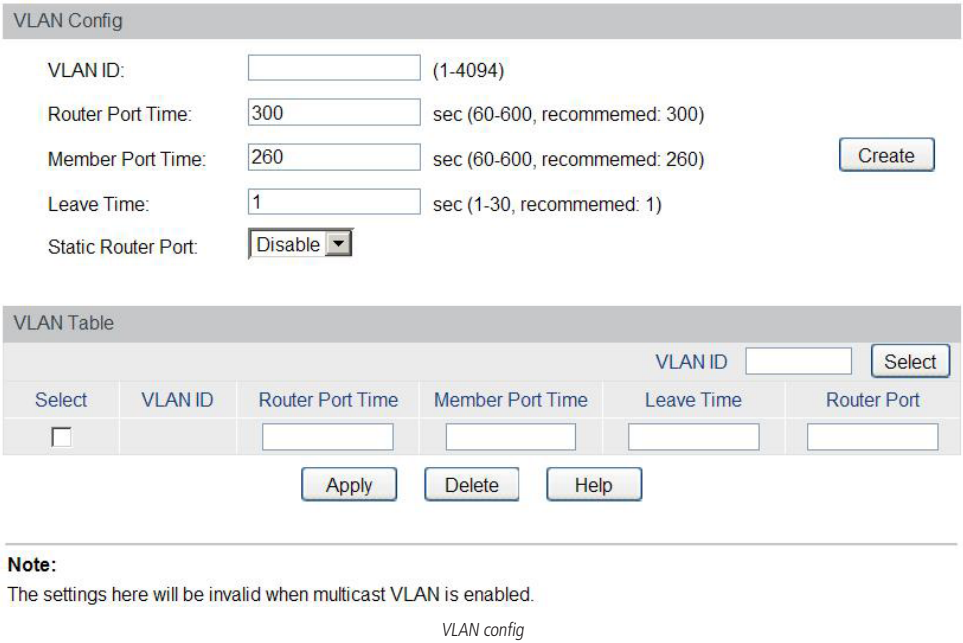
LAG: exibe o número do grupo LAG a qual a porta pertence.

Obs.: *fast Leave somente é suportado na porta do switch quando o cliente utiliza o IGMP v2 ou v3.*

VLAN config

Grupos Multicast estabelecidos com a utilização de IGMP Snooping são baseados em VLANs. Nesta página você pode configurar diferentes parâmetros do IGMP para diferentes VLANs.

Escolha no menu *Multicast* → *IGMP Snooping* → *VLAN Config*, para carregar a seguinte página:



VLAN config

As seguintes opções são exibidas na tela:

» **VLAN config**

VLAN ID: digite a VLAN ID para habilitar o IGMP Snooping na VLAN desejada.

Router port time: especifique o tempo de vida do Router Port. Se o switch não receber mensagens IGMP Query da porta em que o servidor Multicast está conectado dentro de um intervalo de tempo, a porta não será mais considerada como Router Port. O valor padrão é *300* segundos.

Member port time: especifique o tempo de vida do Member Port. Se o switch não receber mensagens IGMP Report da porta em que os membros (cliente) de um grupo Multicast estão conectados dentro de um intervalo de tempo, a porta será removida da Tabela de endereços Multicast. O valor padrão é *260* segundos.

Leave time: especifique o intervalo de tempo entre o switch receber uma mensagem de Leave de um cliente e o servidor Multicast remover o cliente do grupo Multicast. O valor padrão é *1* segundo.

Static router port: selecione a Router Port manualmente.

» **VLAN table**

VLAN ID select: digite a VLAN ID no campo correspondente e clique em *Select* para selecionar a VLAN desejada.

Select: selecione a VLAN ID desejada. Nesta opção é possível selecionar mais de uma VLAN ID simultaneamente.

Router port time: exibe o tempo de vida configurado para o Router Port.

Member port time: exibe o tempo de vida configurado para o Member Port.

Leave time: exibe o Leave Time configurado.

Router port: exibe o número da porta configurado como Router Port.

Obs.: *essas configurações não serão válidas se a função Multicast VLAN estiver habilitada.*

Procedimento de configuração

Passo	Operação	Descrição
1	Habilitar a função IGMP snooping	Obrigatório, Habilitar as configurações globais do IGMP Snooping do switch e das portas em: Multicast⟶IGMP Snooping⟶Snooping Config e Port Config.
2	Configurar os parâmetros de Multicast para as VLANs	Opcional, Configurar os parâmetros Multicast das VLANs em: Multicast⟶IGMP Snooping⟶VLAN Config. Se uma VLAN não tem parâmetros de configuração Multicast, indica que o IGMP Snooping não está habilitado na VLAN, assim os dados Multicast na VLAN serão enviados em broadcast.

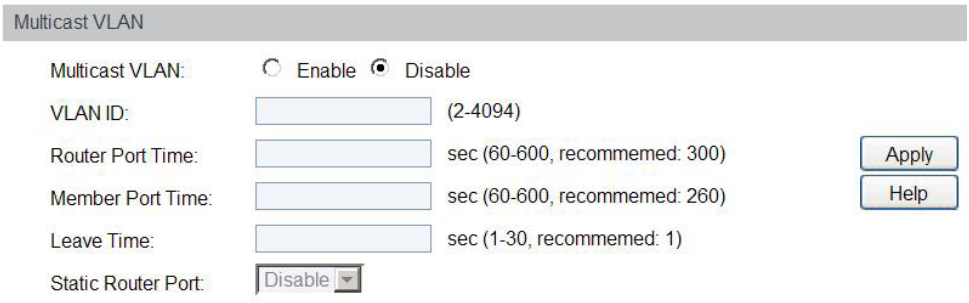
Multicast VLAN

Em transmissões Multicast, quando usuários de diferentes VLANs participam do mesmo grupo Multicast, o servidor Multicast irá duplicar as informações e encaminhará para as VLANs correspondentes, desperdiçando largura de banda e recursos do switch.

Este problema pode ser resolvido por meio do recurso Multicast VLAN. Ao adicionar as portas do switch para Multicast VLAN e habilitar o IGMP Snooping é possível compartilhar a Multicast VLAN entre clientes de diferentes VLANs, economizando largura de banda e recursos do switch, pois os fluxos Multicast são transmitidos somente na Multicast VLAN.

Antes de configurar uma Multicast VLAN é necessário criar uma VLAN (802.1Q) e adicionar as portas correspondentes. Ao ativar uma Multicast VLAN as configurações Multicast das outras VLANs serão desabilitadas, isto é, o tráfego Multicast somente será permitido dentro da Multicast VLAN.

Escolha no menu *Multicast* → *IGMP Snooping* → *Multicast VLAN* para carregar as páginas.



Multicast VLAN

As seguintes opções são exibidas na tela:

» **Multicast VLAN**

Multicast VLAN: selecione *Enable/Disable* para habilitar ou desabilitar a função Multicast VLAN.

VLAN ID: digite o VLAN ID utilizado pelo Multicast VLAN.

Router port time: especifique o tempo de vida do Router Port. Se o switch não receber mensagens IGMP Query da porta em que o servidor Multicast está conectado dentro de um intervalo de tempo, a porta não será mais considerada como Router Port. O valor padrão é *300*.

Member port time: especifique o tempo de vida do Member Port. Se o switch não receber mensagens IGMP Report da porta em que os membros (cliente) de um grupo Multicast estão conectados dentro de um intervalo de tempo, a porta será removida da Tabela de endereços Multicast. O valor padrão é *260* segundos.

Leave time: especifique o intervalo de tempo entre o switch receber uma mensagem de Leave de um cliente e o servidor Multicast remover o cliente do grupo Multicast. O valor padrão é *1* segundo.

Static router port: selecione a Router Port manualmente.

Obs.: *» A porta em que o servidor Multicast estiver conectado ao switch deve estar na Multicast VLAN, caso contrário, os clientes podem não receber o fluxo do Multicast.*

» O Multicast VLAN não terá efeito caso as portas correspondentes não esteja configurado na VLAN (802.1Q) correspondente.

» O modo de funcionamento da porta deverá estar no modo General.

» Configure o modo de funcionamento da porta em que o servidor Multicast está conectado ao switch como TRUNK ou como General com regra de saída TAG, caso contrário, todas as portas membros do Multicast VLAN não receberão tráfego Multicast.

» Depois que uma Multicast VLAN for criada, todos os pacotes IGMP serão processados pela Multicast VLAN.

Procedimentos de configuração

Passo	Operação	Descrição
1	Habilitar a função IGMP Snooping	Obrigatório - Habilitar as configurações globais de IGMP Snooping e de portas em: Multicast ⟶ IGMP Snooping ⟶ Snooping Config e Port Config.
2	Criar a VLAN que será utilizada pelo Multicast VLAN	Obrigatório - Criar a VLAN desejada que será utilizada na Multicast VLAN, adicionando as portas utilizadas pelo tráfego Multicast: VLAN ⟶ 802.1Q VLAN
3	Configura os parâmetros para o Multicast VLAN	Obrigatório - habilitar e configurar a Multicast VLAN Multicast em: Multicast ⟶ IGMP Snooping ⟶ Multicast VLAN. Recomenda-se manter os parâmetros de tempo padrão.
4	Visualizar as configurações	Se for configurado com êxito, o VLAN ID da Multicast VLAN será exibido na tela IGMP Snooping Status em: Multicast⟶IGMP Snooping⟶Snooping Config.

Exemplo de aplicação para Multicast VLAN

» **Requerimentos de rede**

Servidores Multicast enviam fluxos de Multicast através de roteadores e os fluxos são transmitidos para o cliente A e B através do switch.

Roteador: a porta WAN é conectada ao servidor Multicast, a porta LAN é conectada no switch. Os pacotes Multicast são transmitidos na VLAN3.

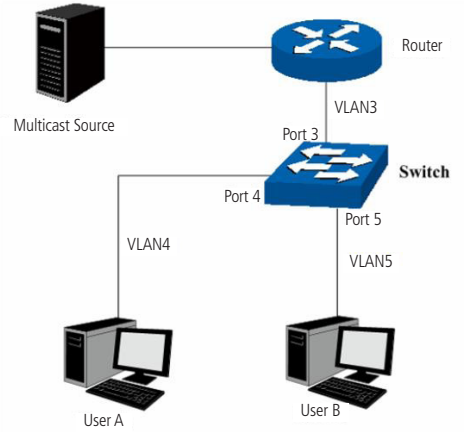
Switch: a porta 3 está conectada ao roteador e os pacotes são transmitidos na VLAN 3; a porta 4 é o cliente A e os pacotes são transmitidos na VLAN 4; a porta 5 está conectada ao cliente B e os pacotes são transmitidos na VLAN 5.

Cliente A: conectado na porta 4 do switch.

Cliente B: conectado na porta 5 do switch.

Configure o Multicast VLAN e os clientes A e B para receberem os fluxos de dados Multicast na Multicast VLAN.

» **Diagrama de rede**



Aplicação Multicast

» **Procedimento de configuração**

Passo	Operação	Descrição
1	Criar VLANs	Crie três VLANs (VLAN 3, 4 e 5 respectivamente) e especifique a descrição da VLAN 3 como Multicast VLAN em: VLAN ⟶ 802.1Q VLAN.
2	Configurar o modo de funcionamento das portas	Configure em: VLAN ⟶ 802.1Q. Para a porta 3, configurar o modo de funcionamento da porta como GENERAL e regra de saída como TAG e adicione-a nas VLAN 3, VLAN 4 e VLAN 5. Para a porta 4, configurar o modo de funcionamento como GENERAL, e regra de saída como UNTAG e adicione-a nas VLAN 3 e VLAN 4. Para a porta 5, configurar o modo de funcionamento como GENERAL, e regra de saída como UNTAG e adicione-a nas VLAN 3 e VLAN 5.
3	Habilitar a função IGMP Snooping	Em Multicast ⟶ IGMP Snooping ⟶ Snooping Config, habilitar globalmente a função IGMP Snooping. Em Multicast ⟶ IGMP Snooping ⟶ Port Config, habilitar o IGMP Snooping para as porta 3, porta 4 e porta 5.
4	Habilitar Multicast VLAN	Em Multicast ⟶ IGMP Snooping ⟶ Multicast VLAN, Habilitar Multicast VLAN e configurar o VLAN ID da Multicast VLAN como 3 e manter os demais parâmetros como padrão.
5	Checar a Multicast VLAN	A Multicast VLAN 3 será exibida na tabela de status do IGMP Snooping em: Multicast ⟶ IGMP Snooping ⟶ Snooping Config

8.2. Multicast IP

Em uma rede, os clientes podem se juntar a diferentes grupos Multicast, dependendo da sua necessidade. O switch encaminha o trafego Multicast com base em sua Tabela de endereços Multicast. O IP Multicast pode ser configurado manualmente nas páginas: *Multicast IP Table, Static Multicast IP*.

Multicast IP table

Nesta página você pode visualizar a Tabela de endereços Multicast do switch.

Escolha no menu: *Multicast* ⟶ *Multicast IP* ⟶ *Multicast IP Table* para carregar a seguinte página.

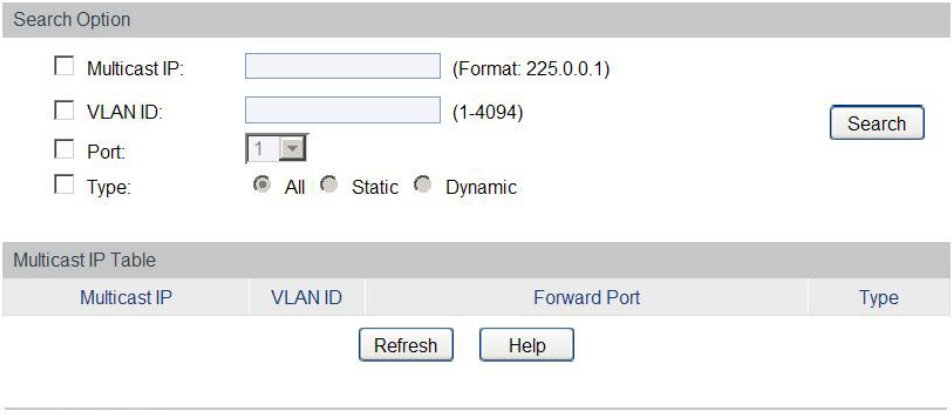


Tabela de endereços Multicast

As seguintes opções são exibidas na tela:

» **Search Option**

Multicast IP: digite endereço IP Multicast desejado para visualizar suas configurações.

VLAN ID: digite o VLAN ID para visualizar as configurações Multicast pertence à VLAN desejada.

Port: selecione o número da porta desejada.

Type: selecione o tipo da entrada desejada.

» All: exibe todas as entradas de endereços IP Multicast.

» Static: exibe todos os endereços IPs Multicast estático.

» Dynamic: exibe todos os endereços IPs Multicast dinâmicos.

» **Multicast IP table**

Multicast IP: exibe o endereço IP Multicast.

VLAN ID: exibe a VLAN ID do grupo Multicast.

Forward port: exibe as portas participantes do grupo Multicast.

Type: exibe o tipo de IP Multicast.

Obs.: *caso as configurações de VLANs e Multicast VLAN forem alteradas, o switch irá renovar os endereços dinâmicos na Tabela de endereços Multicast e aprenderá os novos endereços Multicast.*

Static Multicast IP

Nesta página é possível configurar a Tabela de endereços Multicast manualmente. Esta tabela funciona de modo isolado em relação ao grupo Multicast dinâmico e do filtro Multicast. Estes endereços não são aprendidos pelo IGMP Snooping, desta forma é possível melhorar a qualidade e segurança dos dados Multicast transmitidos na rede.

Escolha no menu *Multicast* → *Multicast IP* → *Static Multicast IP* para carregar a seguinte página:

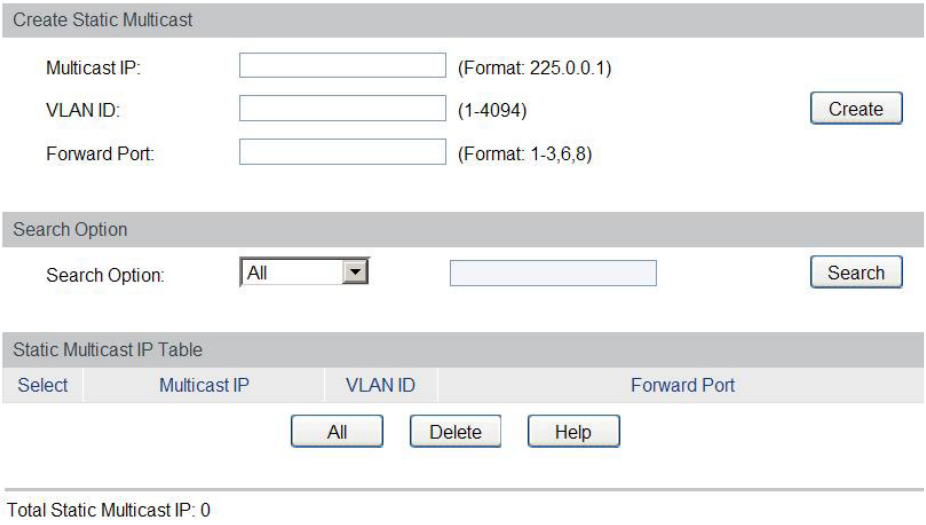


Tabela de endereços Multicast estática

As seguintes opções são exibidas na tela:

» **Create static Multicast**

Multicast IP: digite o endereço IP Multicast desejado para adicioná-lo na Tabela de endereços Multicast Estático.

VLAN ID: digite a VLAN ID que pertence o endereço IP Multicast.

Forward port: digite as portas de encaminhamento utilizado pelo grupo Multicast. Utilize o formato (1-3, 6, 9).

» **Search option**

Search option: selecione o modo de pesquisa desejado para exibição da Tabela de endereços Multicast Estático e clique em *Search*.

» All: exibe todos os endereços da Tabela de endereços Multicast Estáticos.

» Multicast IP: digite o endereço IP Multicast para visualizar a entrada correspondente da Tabela de endereços Multicast Estático.

» VLAN ID: digite o VLAN ID para visualizar a entrada correspondente utilizada pela Tabela de endereços Multicast Estático.

» Port: digite o número da porta desejada para visualizar os endereços da Tabela de endereços Multicast Estático.

» **Static Multicast IP table**

Select: selecione o endereço IP Multicast desejado e clique no botão *Delete* para removê-lo da Tabela de endereços Multicast Estático. Nesta opção é possível selecionar mais de uma entrada simultaneamente.

Multicast IP: exibe o endereço IP Multicast.

VLAN ID: exibe a VLAN ID do Grupo Multicast.

Forward port: exibe as portas de encaminhamento utilizado pelo grupo Multicast.

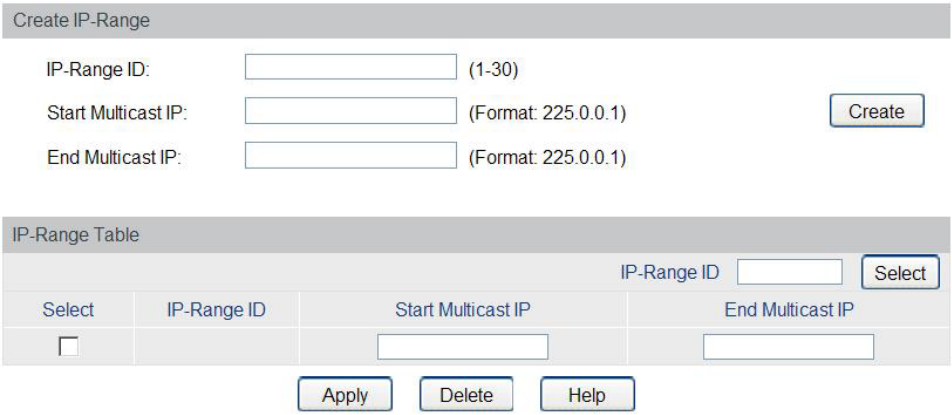
8.3. Multicast filter

Quando o IGMP Snooping é habilitado, é possível especificar uma faixa de endereços IP Multicast que serão permitidos ou negados de serem adicionados na Tabela de endereços Multicast. Ao solicitar um grupo Multicast, o cliente envia uma mensagem IGMP Report, após receber a mensagem o switch irá em primeiro lugar, verificar as regras de filtragem de Multicast configurado na porta de recebimento. Se a porta pode ser adicionada ao grupo Multicast, ela será adicionada a Tabela de endereços Multicast, se a porta não pode ser adicionada ao grupo de Multicast, o switch irá bloquear a mensagem IGMP Report. Desta forma, impedindo a associação do cliente ao grupo Multicast.

IP-Range

Nesta página é possível configurar e visualizar a faixa de endereços IP Multicast utilizados pela função Multicast Filter.

Entre no menu *Multicast* → *Multicast Filter* → *IP-Range* para carregar a seguinte página:



Faixa de endereços Multicast

As seguintes opções são exibidas na tela:

» **Create IP-Range**

IP Range ID: digite o ID da faixa de endereços Multicast que será criado.

Start Multicast IP: digite o endereço IP Multicast inicial utilizados pela faixa de endereços que será criada.

End Multicast IP: digite o endereço IP Multicast final utilizados pela faixa de endereços que será criada.

Create: clique no botão *Create*, para criar a faixa de endereços.

» **IP-Range table**

IP-Range ID select: digite o ID da faixa de endereços Multicast e clique no botão *Select* para selecionar a faixa desejada.

Select: selecione a entrada desejada para apagar ou modificar a faixa de endereços Multicast correspondente. Nesta opção é possível selecionar mais de uma faixa simultaneamente.

IP-Range ID: exibe o ID de identificação da faixa de endereços Multicast.

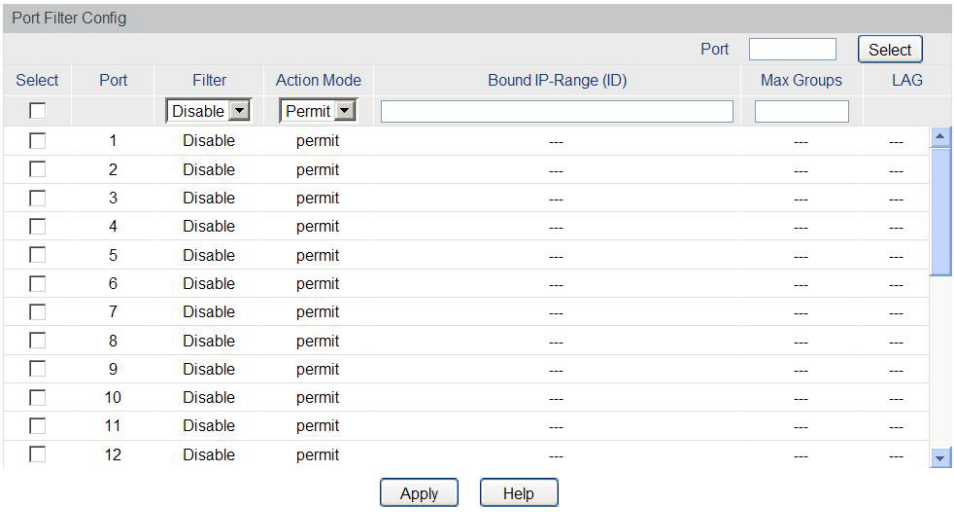
Start Multicast IP: exibe o endereço IP Multicast inicial da faixa criada.

End Multicast IP: exibe o endereço IP Multicast final da faixa criada.

Port filter

Nesta página é possível configurar as regras de Filtro Multicast para cada porta do switch.

Escolha o menu *Multicast* → *Multicast Filter* → *Port Filter* para carregar a seguinte página.



Note:

1. The port filter configuration here has no effect on static multicast IP.
2. Up to 15 IP-Ranges can be bound to one port. Please input the Bound IP-Range (ID) in the format like: 1,5,8.

Filtro Multicast

As seguintes opções são apresentadas na tela:

» **Port filter config**

Port select: digite a porta deseja no campo correspondente e clique em Select para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Filter: selecione *Enable/Disable* para habilitar ou desabilitar função de filtro Multicast na porta desejada.

Action mode: selecione o modo como o switch irá processar os pacotes Multicast quando o endereço IP Multicast estiver dentro da faixa de endereços:

» Permit: apenas os pacotes Multicast que possuem endereço IP Multicast dentro da faixa configurada serão encaminhados pelo switch.

» Deny: apenas os pacotes Multicast, que possuem endereço IP Multicast dentro da faixa configurada serão descartados pelo switch.

Bound IP-Range (ID): digite o ID da faixa de endereços Multicast que a porta será vinculada.

Max groups: especifique o número máximo de grupos Multicast, para evitar que algumas portas utilizem muita largura de banda.

LAG: exibe o número do grupo LAG que a porta pertence.

Obs.: » *A função de Filtro Multicast somente funcionará em uma VLAN com IGPM Snooping habilitado.*

» *A função de Filtro Multicast não terá efeito sobre Multicast IP Estático.*

» *Pode ser configurado até 5 faixas de endereços Multicast em cada porta. Utilize o formato: 1, 5, 8.*

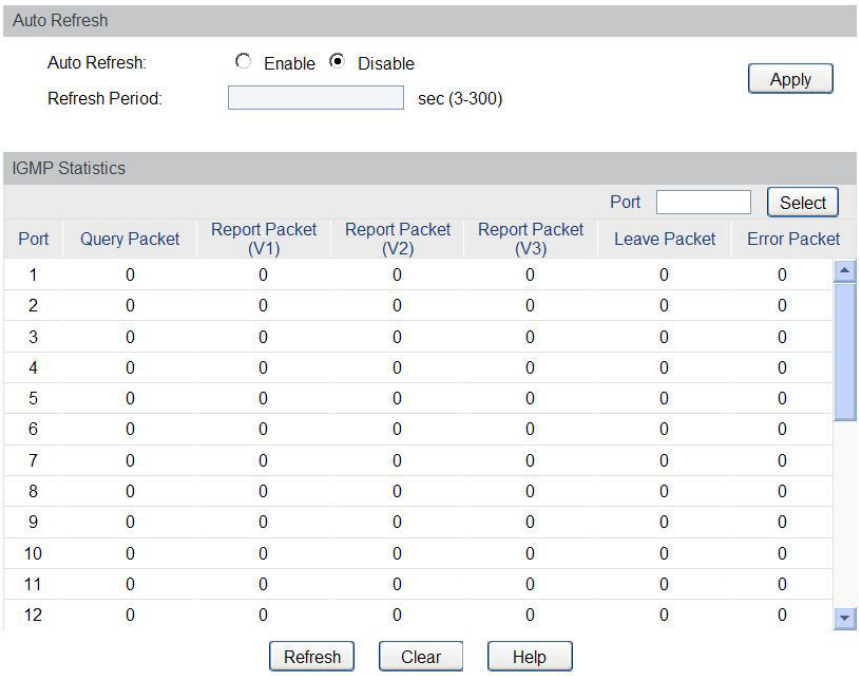
Procedimento de configuração

Passo	Operação	Descrição
1	Configure a faixa de endereços IP Multicast que será utilizada pelo Filtro Multicast.	Obrigatório, Configure a faixa de endereços que será filtrado: Multicast ⟶ Multicast Filter ⟶ IP Range
2	Configure as regras de Filtro Multicast para cada porta do switch.	Obrigatório, Configure as regras de Filtro Multicast para as portas: Multicast ⟶ Multicast Filter ⟶ Port Filter

8.4. Packet statistics

Nesta página você pode visualizar o tráfego de dados Multicast em cada porta do switch, o que facilita o monitoramento de mensagens IGMP na rede.

Escolha no menu *Multicast → Packet Statistics* para carregar a seguinte página:


Auto Refresh
Auto Refresh: Enable Disable
Apply
Refresh Period: sec (3-300)
IGMP Statistics
Port Select
Port Query Packet Report Packet (V1) Report Packet (V2) Report Packet (V3) Leave Packet Error Packet
1 0 0 0 0 0 0
2 0 0 0 0 0 0
3 0 0 0 0 0 0
4 0 0 0 0 0 0
5 0 0 0 0 0 0
6 0 0 0 0 0 0
7 0 0 0 0 0 0
8 0 0 0 0 0 0
9 0 0 0 0 0 0
10 0 0 0 0 0 0
11 0 0 0 0 0 0
12 0 0 0 0 0 0
Refresh Clear Help

Estatísticas dos pacotes IGMP

As seguintes opções são exibidas na tela:

» **Auto refresh**

Auto refresh: selecione *Enable/Disable* para habilitar ou desabilitar a função de refresh automático.

Refresh period: digite um tempo de 3 a 300 segundos, para especificar o período de atualização automática.

» **IGMP statistics**

Port select: digite a porta deseja no campo correspondente e clique em *Select* para selecionar a porta.

Port: exibe o número da porta.

Query packet: exibe o número de pacotes IGMP Query que a porta recebeu.

Report packect (V1): exibe o número de pacotes IGMP Report v1 que a porta recebeu.

Report packect (V2): exibe o número de pacotes IGMP Report v2 que a porta recebeu.

Report packect (V3): exibe o número de pacotes IGMP Report v3 que a porta recebeu.

Leave packet: exibe o número de pacotes IGMP Leave que a porta recebeu.

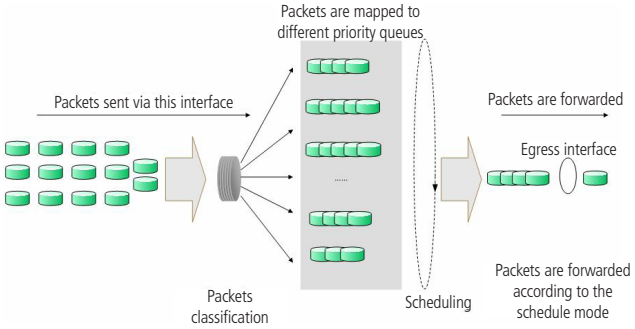
Error packet: exibe o número de pacotes IGMP Error que a porta recebeu.

9. QoS

A função QoS (Quality of Service) é utilizada para fornecer qualidade de serviço a vários requisitos e aplicações utilizados na rede, otimizando e distribuindo a largura de banda.

» **QoS**

Este switch classifica e mapeia os pacotes entrantes e coloca-os em diferentes filas de prioridades, em seguida encaminha os pacotes de acordo com o algoritmo de escalonamento selecionado, implementando a função de QoS.


Packets are mapped to different priority queues
Packets sent via this interface
Packets are forwarded
Egress interface
Packets are forwarded according to the schedule mode
Packets classification
Scheduling

QoS

» Traffic classification: identifica pacotes em conformidades com determinadas regras.

» Map: o usuário pode mapear os pacotes entrantes para filas de prioridades diferentes, com base nos modelos de prioridade. Este switch implementa três modelos de prioridades: *Prioridade por Porta, 802.1P* e *DSCP*.

» Queue scheduling algorithm: o switch suporta quatro modelos de algoritmos de escalonamento: *SP, WRR, SP+WRR* e *Equ.*

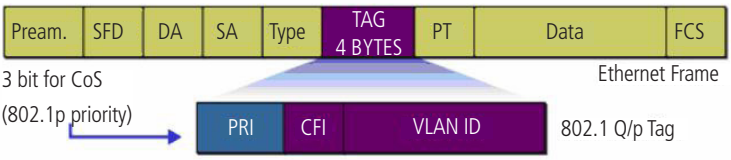
» **Priority mode**

O switch implementa três modelos de prioridades, baseada em porta, 802.1p e DSCP. Por padrão, o modo de prioridade baseada em portas vem ativado e os demais modos são opcionais.

1. Port Priority

Port Priority é a configuração de prioridade por porta. O fluxo de dados será mapeado para as filas de saída conforme a regra de CoS definido para cada porta.

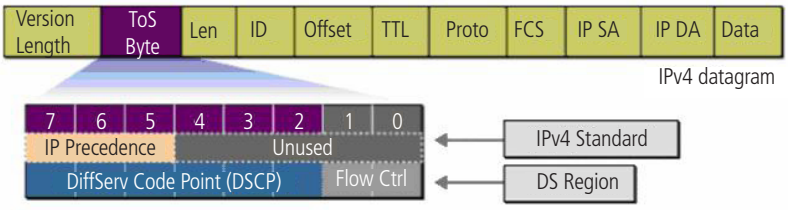
2. 802.1P Priority



TAG 802.1Q

De acordo com a figura anterior, cada TAG 802.1Q inserida no quadro Ethernet possui um campo chamado *PRI*, este campo, possui 3 bits que são utilizados para a classificação e priorização do pacote, sendo possível configurar até 8 níveis de priorização (0 a 7). Na página de gerenciamento web, é possível mapear diferentes níveis de priorização de acordo com a fila de prioridade desejada. O switch processa os pacotes não marcados (*untagged*) com base no modo de prioridade padrão.

3. DSCP Priority



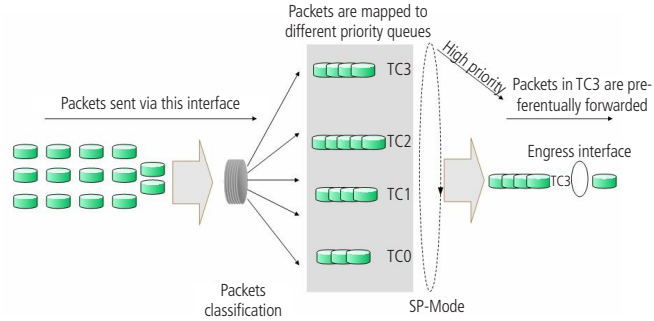
Datagrama IP

De acordo com a figura acima, o campo *ToS* (Type Of Service) do cabeçalho IP possui 1 byte, ou seja 8 bits. Os três primeiros bits indicam a Precedência IP e variam dentro do intervalo que vai de 0 a 7, os cinco bits restantes não são utilizados. A RFC 2474 redefiniu o campo ToS do datagrama IP, chamando-o de campo *DS* (Differentiated Service), deste modo, os 6 primeiros bits mais significativos (bit 7 ao bit 2), diferenciam os pacotes recebidos em classes de tráfego, conforme informações de atraso, processamento e confiabilidade, os dois últimos bits menos significativos (bit 1 e bit 0) são reservados. É possível configurar até 64 classes de tráfego DSCP, este intervalo é configurado dentro da faixa que vai de 0 a 63.

» **Schedule mode**

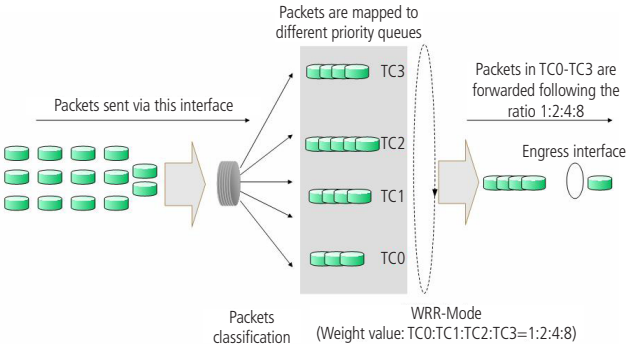
Quando a rede está congestionada, muitos pacotes podem ser perdidos ou chegarem com atrasos em seus destinos, ocasionando lentidão e prejudicando os serviços utilizados pela rede. Estes problemas podem ser resolvidos com a utilização de algoritmos de escalonamento. O switch implementa 4 filas de prioridade: *TC0, TC1, TC2* e *TC3*. TC0 tem a menor prioridade, enquanto TC3 tem a maior prioridade, que são implementados com os seguintes algoritmos de escalonamento: *SP, WRR, SP+WRR* e *Equ*.

1. SP: algoritmo *SP* (Strict Priority). Neste modo, a fila com maior prioridade ocupará totalmente a largura de banda. Os pacotes em fila de menor prioridade somente serão enviados após todos os pacotes de filas com maior prioridade serem enviados. O switch possui 4 filas de prioridades definidos como: *TC0, TC1, TC2, TC3*, quanto maior o valor da fila, maior a prioridade. A desvantagem de se utilizar o algoritmo de escalonamento de filas SP é que caso ocorra um congestionamento de pacotes em filas com maiores prioridades, os pacotes em filas de menores prioridades não serão atendidos.



Algoritmo SP

2. WRR: algoritmo *WRR* (Weight Round Robin). Neste modo, os pacotes de todas as filas serão enviados de acordo com o peso de cada fila, este peso indica a proporção ocupada pelo recurso. As filas de prioridades são atendidas em ordem pelo algoritmo WRR, caso uma fila estiver vazia, o algoritmo passa para a próxima fila. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2, TC3 = 1:2:4:8.



Algoritmo WRR

3. SP+WRR: Algoritmo *SP+WRR*. Neste modo, o switch faz a priorização das filas através do uso dos dois algoritmos de escalonamento (SP e WRR). A fila TC3 pertence ao grupo SP, isto é, a fila ocupará toda a largura de banda até que não possua mais pacotes a serem enviados, enquanto as os pacotes das filas TC0, TC1 e TC2 serão atendidos conforme o peso de cada fila utilizando o algoritmo WRR, a relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1 e TC2 = 1:2:4.
4. Equ-Mode: neste modo, todas as filas ocupam igualmente a largura de banda. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:1:1:1.

O menu Qos inclui três sub-menus: *DiffServ, Bandwidth Control* e *Voice VLAN*.

9.1. DiffServ

O switch classifica os pacotes de ingresso, mapeando para diferentes filas de prioridades e em seguida encaminha os pacotes de acordo com o algoritmo de escalonamento selecioando pela função QoS.

Este switch implementa três modos de prioridades, baseada em portas, em 802.1P e DSCP e suporta quatro algoritmos de escalonamento.

As prioridades baseadas em portas são rotuladas como CoS0, CoS1... CoS7.

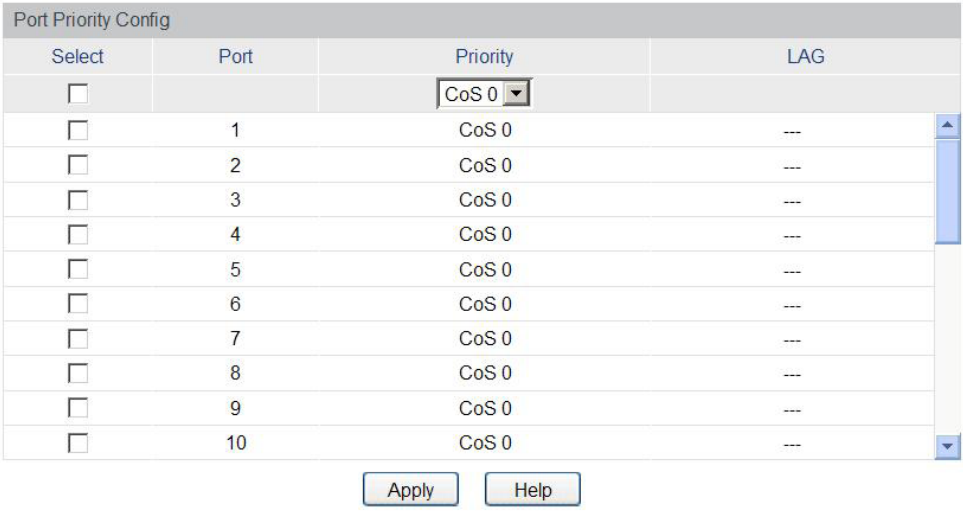
O DiffServ pode ser configurado nas páginas de configuração *Port Priority, Schedule Mode, 802.1P Priority* e *DSCP Priority*.

Port priority

Nesta página você pode configurar a prioridade das portas.

Quando a prioridade por porta é especificada, os pacotes serão classificados com base no valor do CoS da porta de entrada e enviados para as filas de prioridade conforme a relação de mapeamento configurado entre o CoS e o TC nas configurações 802.1P.

Escolha o menu *QoS* → *DiffServ* → *Port Priority* para carregar a seguinte página:


Port Priority Config
Select
Port
Priority
LAG
CoS 0
1 CoS 0 ---
2 CoS 0 ---
3 CoS 0 ---
4 CoS 0 ---
5 CoS 0 ---
6 CoS 0 ---
7 CoS 0 ---
8 CoS 0 ---
9 CoS 0 ---
10 CoS 0 ---
Apply
Help
note:
Port priority is one property of the port. When the port priority is specified, the data will be classified into the egress queue based on the CoS value of the ingress port and the mapping relation between the CoS and TC in 802.1P.

Prioridade por porta

As seguintes opções são exibidas na tela:

» **Port priority config**

Select: selecione as portas desejadas para configurar a prioridade.

Port: exibe o número físico da porta no switch.

Priority: selecione a prioridade para a porta.

LAG: exibe o número do grupo LAG a qual a porta pertence

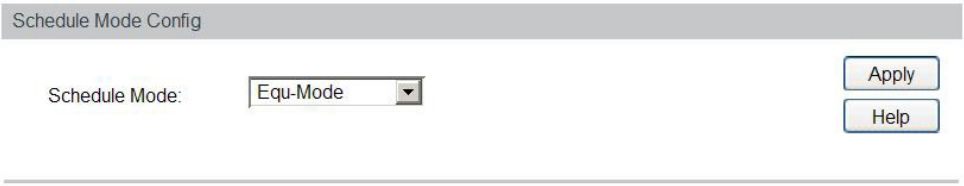
Procedimento de configuração

Passo	Operação	Descrição
1	Selecione a prioridade da porta	Obrigatório, QoS ⟶ DiffServ ⟶ Port Priority, para configurar a prioridade da porta.
2	Configure a relação de mapeamento entre a prioridade 802.1P e a fila de prioridade (TC).	Obrigatório, QoS ⟶ Diff Serv ⟶ 802.1P Priority, configure o mapeamento entre 802.1P e a fila de prioridade (TC).
3	Selecione o modo de agendamento	Obrigatório, QoS ⟶ DiffServ ⟶ Schedule, selecione o modo de agendamento.

Schedule mode

Nesta página é possível configurar até 4 tipos de algoritmos de escalonamento. Estes algoritmos são responsáveis pela ordem de encaminhamento dos pacotes que estão dentro de diferentes filas de prioridade.

Escolha o menu *QoS ⟶ DiffServ ⟶ Schedule Mode* para carregar a página seguinte:



Algoritmo de escalonamento

» **Schedule mode config**

SP-Mode: algoritmo SP (Strict Priority). Neste modo, a fila com maior prioridade ocupará totalmente a largura de banda. Os pacotes em fila de menor prioridade somente serão enviados após todos os pacotes de filas com maior prioridade serem enviados. O switch possui 4 filas de prioridades definidos como: *TC0, TC1, TC2, TC3*, quanto maior o valor da fila, maior a prioridade. A desvantagem de se utilizar o algoritmo de escalonamento de filas SP é que caso ocorra um congestionamento de pacotes em filas com maiores prioridades, os pacotes em filas de menores prioridades não serão atendidos.

WRR-Mode: algoritmo WRR (Weight Round Robin). Neste modo, os pacotes de todas as filas serão enviados de acordo com o peso de cada fila, este peso indica a proporção ocupada pelo recurso. As filas de prioridades são atendidas em ordem pelo algoritmo WRR, caso uma fila estiver vazia, o algoritmo passa para a próxima fila. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2, TC3 = 1:2:4:8.

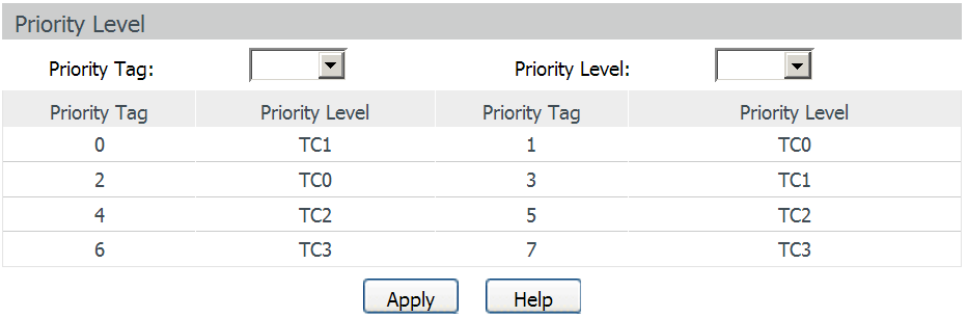
SP+WRR-Mode: algoritmo SP+WRR. Neste modo, o switch faz a priorização das filas através do uso dos dois algoritmos de escalonamento (SP e WRR). A fila TC3 pertence ao grupo SP, isto é, a fila ocupará toda a largura de banda até que não possua mais pacotes a serem enviados, enquanto os pacotes das filas TC0, TC1 e TC2 serão atendidos conforme o peso de cada fila utilizando o algoritmo WRR, a relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1 e TC2 = 1:2:4.

Equal-Mode: neste modo, todas as filas ocupam igualmente a largura de banda. A relação de prioridade das filas com o peso de cada fila, seguem a ordem: TC0, TC1, TC2 e TC3 = 1:1:1:1.

802.1P Priority

Nesta página é possível configurar a prioridade 802.1P. O switch analisa a TAG de VLAN que foi inserido no quadro Ethernet do pacote enviado. Esta TAG possui um campo chamado PRI de 3 bits que são utilizados para a classificação e priorização do pacote, sendo possível configurar até 8 níveis de priorização (0 a 7).

Escolha o menu *QoS → DiffServ → 802.1P Priority* para carregar a seguinte página:



Prioridade 802.1P

As seguintes opções são apresentadas na tela:

» **Priority level**

Priority tag: selecione a prioridade definida pelo IEEE802.1p.

Priority level: selecione a a fila de saída em que o pacote com prioridade 802.1p será relacionado. Existem 4 filas, variando de 0 a 3, representados como *TC0, TC1, TC2, TC3*, quanto maior o valor da fila, maior a prioridade.

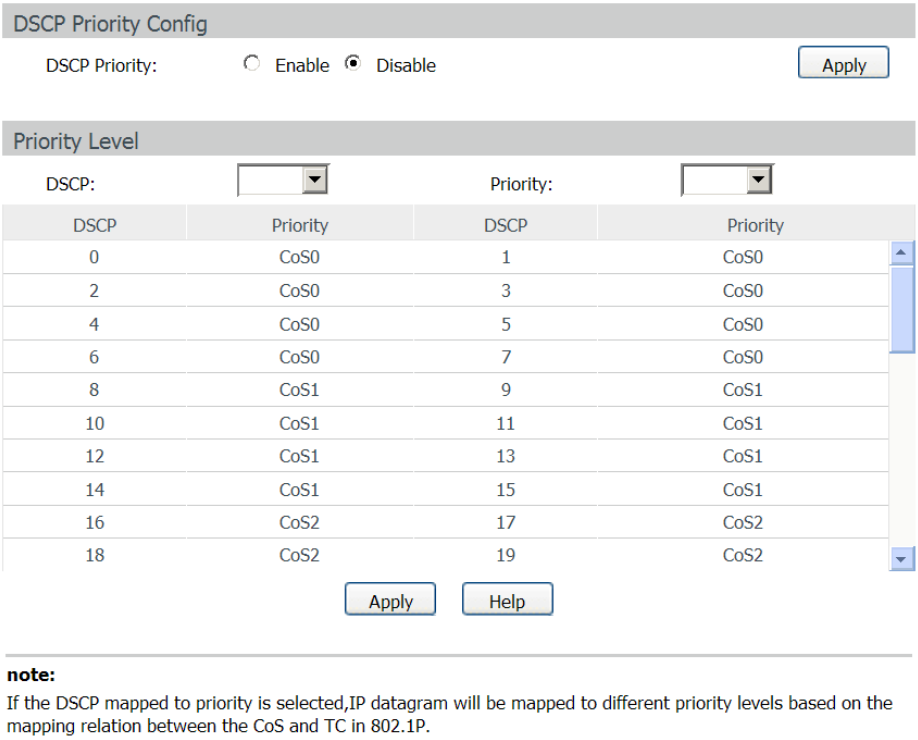
Procedimento de configuração:

Passo	Operação	Descrição
1	Configurar a relação de mapeamento entre 802.1P e a fila de prioridade (TC)	Obrigatório, QoS ⟶ DiffServ ⟶ 802.1P Priority, configure a relação de mapeamento entre a 802.1P e a fila de prioridade (TC).
2	Selecionar o algoritmo de escalonamento	Obrigatório, QoS ⟶ DiffServ ⟶ Schedule, selecione o algoritmo de escalonamento.

DSCP priority

Nesta página é possível configurar a *Prioridade DSCP*. O switch analisa o campo ToS (Type Of Service) do cabeçalho IP. Este campo possui 1 byte (8 bits) de tamanho, os 6 primeiros bits mais significativos diferenciam os pacotes recebidos em classes de tráfego, conforme informações de atraso, processamento e confiabilidade, os dois últimos bits menos significativos são reservados. É possível configurar até 64 classes de tráfego DSCP, este intervalo é configurado dentro da faixa que vai de 0 a 63.

Escolha o menu *QoS ⟶ DiffeServ ⟶ DSCP Priority* para carregar a seguinte página:



Prioridade DSCP

As seguintes opções são exibidas na tela:

» **DSCP priority config**

DSCP priority: selecione *Enable/Disable* para habilitar ou desabilitar a prioridade DSCP.

» **Priority level**

DSCP: selecione a prioridade determinada pela região DS do datagrama IP. Varia de 0 a 63.

Priority: selecione a prioridade CoS. Os pacotes serão classificados com base no valor DSCP da porta de entrada e enviados para as filas de prioridade conforme relação de mapeamento configurado entre o CoS e o TC nas configurações 802.1P.

Procedimento de configuração

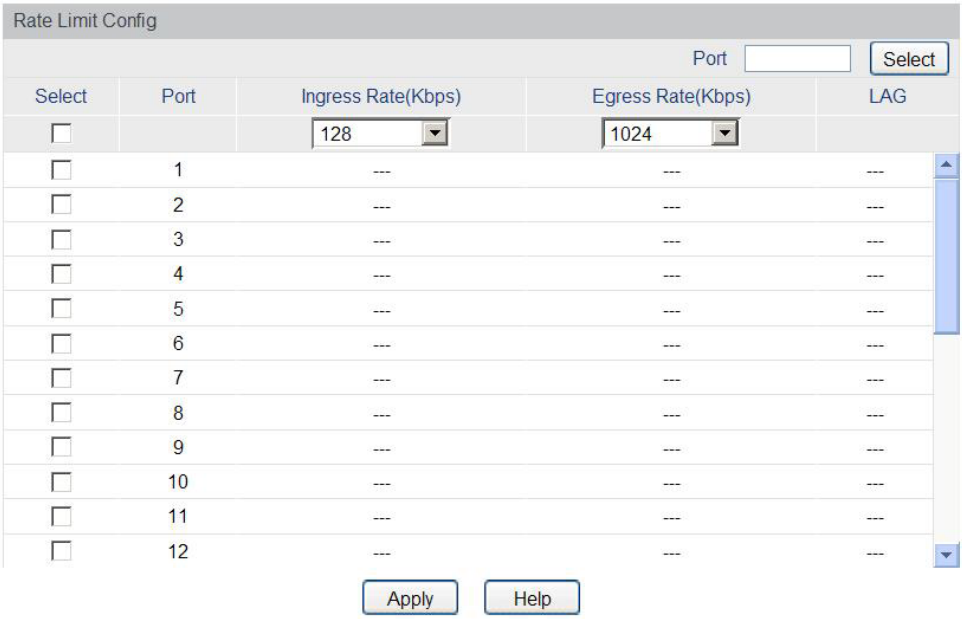
Passo	Operação	Descrição
1	Configure a relação de mapeamento entre o DSCP e 802.1P	Obrigatório, QoS ⟶ DiffServ⟶ DSCP Priority, habilitar a prioridade DSCP e configurar a relação de mapeamento entre a prioridade DSCP e 802.P
2	Configurar a relação de mapeamento entre 802.1P e a fila de prioridade (TC)	Obrigatório, QoS ⟶ DiffServ ⟶ DSCP Priority, configurar a relação de mapeamento entre a prioridade 802.1P e a fila de prioridade (TC).
3	Selecione o algoritmo de escalonamento	Obrigatório, QoS ⟶ DiffServ⟶ Schedule, selecione o algoritmo de escalonamento.

9.2. Bandwidth control

A função de Bandwidth Control, permite que você controle a largura de banda e o fluxo de transmissão de cada porta, sendo configurados nas seguintes páginas: *Rate Limit* e *Storm Control*.

Rate limit

Rate Limit é utilizado para controlar a taxa do tráfego de entrada e de saída dos pacotes para cada porta.



Note:

1. For one port, you cannot enable the Storm Control and the Ingress rate control at the same time.
2. If you select "Manual" to set Ingress/Egress rate, the system will automatically select integral multiple of 64Kbps that closest to the rate you entered as the real Ingress/Egress rate.

Controle de tráfego

As seguintes opções são exibidas na tela:

» **Rate limit config**

Port select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta desejada.

Select: selecione a porta desejada. Neste menu você poderá selecionar um ou mais portas.

Port: exibe o número da porta do switch.

Ingress Rate (Kbps): selecione a largura de banda para recebimento de pacotes na porta.

Egress Rate (Kbps): selecione a largura de banda para envio de pacotes na porta.

LAG: exibe o número do grupo LAG que a qual a porta pertence.

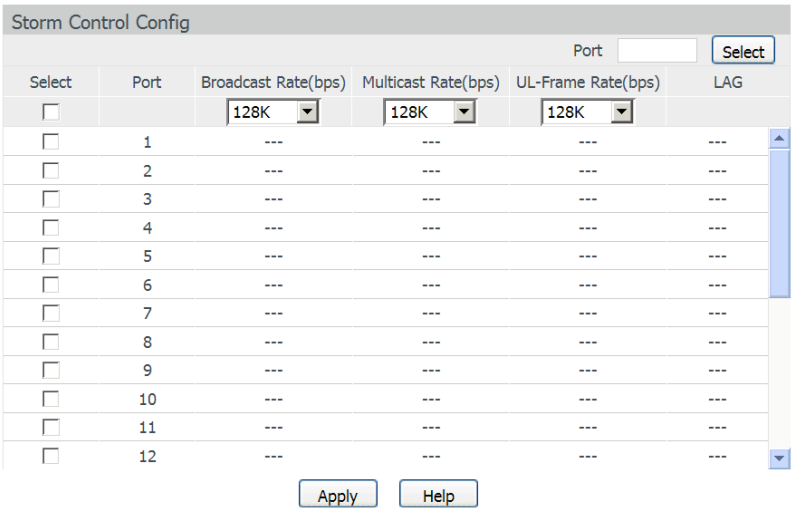
Obs.: » *Se habilitar a função Ingress Rate com a função Storm Control habilitada, o Storm Control será desabilitado para a porta específica.*

» *Quando habilitar a função Egress Rate para uma ou mais portas, é desejável que se desabilite o controle de fluxo das portas para garantir que o switch funcione normalmente.*

Storm control

A função *Storm Control* permite que o switch filtre por porta os pacotes do tipo broadcast, Multicast e UL Frames (pacotes sem endereço IP definido). Se a taxa de transmissão de algum dos três tipos de pacotes excederem a largura de banda configurada, os pacotes serão rejeitados automaticamente, evitando assim tempestade de broadcast na rede.

Escolha o menu *QoS → Bandwitdth Control → Storm Control* para carregar a seguinte página:



Storm control

As seguintes opções são exibidas na tela:

» **Storm control config**

Port select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta desejada.

Select: selecione a porta desejada. Neste menu você poderá selecionar um ou mais portas.

Port: exibe o número de porta do switch.

Broadcast Rate (bps): selecione a largura de banda para receber pacotes de broadcast na porta. O tráfego de pacotes superior a largura de banda serão descartados. Selecione *Disable* para desativar a função de Storm Control para a porta.

Multicast Rate (bps): selecione a largura de banda para receber pacotes de Multicast na porta. O tráfego de pacotes superior a largura de banda serão descartados. Selecione *Disable* para desativar a função de Storm Control para a porta.

UL-Frame Rate (bps): selecione a largura de banda para receber pacotes de UL-Frames na porta. O tráfego de pacotes superior a largura de banda serão descartados. Selecione *Disable* para desativar a função de Storm Control para a porta.

Lag: exibe o número do grupo LAG a qual a porta pertence.

Obs.: *se habilitar a função Ingress Rate com a storm control habilitado, o storm control será desabilitado para a porta específica.*

9.3. Voice VLAN

Voice VLANs são configuradas especialmente para o fluxo de dados de voz. Ao configurar VLANs de voz e adicionar as portas a dispositivos de voz, você pode executar QoS relacionando as configurações de dados e voz, garantindo a prioridade de transmissão dos fluxos de dados e a qualidade da voz.

» **Endereço OUI (Organizationally Unique Identifier)**

O switch pode determinar se um pacote é ou não de voz, marcando seu endereço MAC de origem. Se a origem do endereço MAC corresponde a algum OUI configurado no sistema, os pacotes são determinados como pacotes de voz e serão transmitidos na VLAN de voz.

Um endereço OUI, é um identificador único atribuído pela IEEE (Institute of Electrical and Electronics Engineers) para um fornecedor de dispositivos. Ele compreende os 24 primeiros bits de um endereço MAC. Você pode reconhecer a qual fornecedor um dispositivo pertence de acordo com o endereço OUI. A tabela a seguir, mostra os endereços OUI de vários fabricantes que já estão pré-definidos no switch.

Number	Endereço OUI	Fabricante
1	00-01-E3-00-00-00	Siemens Phone
2	00-03-6B-00-00-00	Cisco Phone
3	00-04-0D-00-00-00	Avaya Phone
4	00-60-B9-00-00-00	Philips/NEC Phone
5	00-D0-1E-00-00-00	Pingtel Phone
6	00-E0-75-00-00-00	Polycom Phone
7	00-E0-BB-00-00-00	3COM Phone

» **Modos da porta Voice VLAN**

A VLAN de voz pode operar em dois modos: Automático e Manual.

Automatic Mode: neste modo o switch adiciona automaticamente a porta que recebe os pacotes de voz para a VLAN de Voz através do aprendizado do endereço MAC de origem do dispositivo e determina a prioridade dos pacotes enviados não marcados (untagged).

O tempo de envelhecimento (aging time) das portas pertencentes a VLAN de Voz podem ser configurados no switch. Se o switch não receber qualquer pacote de voz correspondente durante o intervalo especificado, a porta será removida da VLAN de Voz. Portas de voz são automaticamente adicionados ou removidos na VLAN de Voz.

Manual Mode: neste modo, será necessário adicionar manualmente a porta em que o dispositivo de voz está conectado para ser membro da VLAN de Voz e atribuir regras de ACL para configurar as prioridades dos pacotes conforme os endereços MAC de origem e OUI correspondentes.

Na prática, a porta participante de uma VLAN de Voz é configurada de acordo com o tipo dos pacotes enviados partir de um dispositivo de voz e do modo de funcionamento da porta. A tabela a seguir mostra informações detalhadas.

Modo da porta	Tipo dos dados de voz	Modo de funcionamento e procesamento da porta
Automatic	Pacotes de voz TAGGED	ACCESS: não suportado.
		TRUNK: suportado, a VLAN padrão da porta não pode ser Voice VLAN.
		GENERAL: suportado, a VLAN padrão da porta não pode ser Voice VLAN e a regra de saída da porta de acesso a VLAN padrão deve ser TAG.
	Pacotes de voz UNTAGGED	ACCESS, TRUNK, GENERAL: não suportados.
Manual	Pacotes de voz TAGGED	ACCESS: não suportado.
		TRUNK: suportado. A VLAN padrão da porta deve ser Voice VLAN.
		GENERAL: suportado. A VLAN padrão da porta não pode ser Voice VLAN e a regra de saída da porta de acesso a VLAN padrão deverá ser TAG.
	Pacotes de voz UNTAGGED	ACCESS: suportado. A VLAN padrão da porta deve ser Voice VLAN.
		TRUNK: suportado. A VLAN padrão da porta deve ser a Voice VLAN e a porta deve permitir acesso de pacotes da Voice VLAN.
		GENERAL: suportado. A VLAN padrão da porta não deve ser Voice VLAN e a regra de saída da porta de acesso a VLAN padrão deve ser UNTAG.

» **Modo de segurança das portas Voice VLAN**

Quando a Voice VLAN estiver habilitada para uma porta, você pode habilitar a opção Modo de Segurança da porta, para filtrar fluxos de dados.

Se o modo de segurança estiver habilitado, a porta apenas encaminha os pacotes de voz, e descarta os outros pacotes cujo endereço MAC de origem não corresponda ao endereço OUI configurado. Se o modo de segurança estiver desabilitado, a porta encaminha todos os pacotes recebidos.

Modo de segurança	Tipo de pacote	Modo de funcionamento e processamento da porta
Enable	Pacotes UNTAGGED	Quando o endereço MAC de origem do pacote corresponder com o endereço OUI configurado, o pacote poderá ser transmitido na Voice VLAN. Caso contrário, o pacote será descartado.
	Pacotes de voz TAGGED	
	Pacotes de dados TAGGED	Quando o endereço MAC de origem do pacote corresponder com o endereço OUI configurado, o pacote poderá ser transmitido na Voice VLAN. Caso contrário, o pacote será descartado.
Disable	Pacotes UNTAGGED	Não verifica o endereço MAC de origem dos pacotes e todos os pacotes podem ser transmitidos na Voice VLAN.
	Pacotes de voz TAGGED	
	Pacotes de dados TAGGED	O modo de processamento para os pacotes de dados marcados, será determinado pelo fato da porta permitir ou não a transmissão do pacote na VLAN correspondente, independente do modo de segurança configurado.

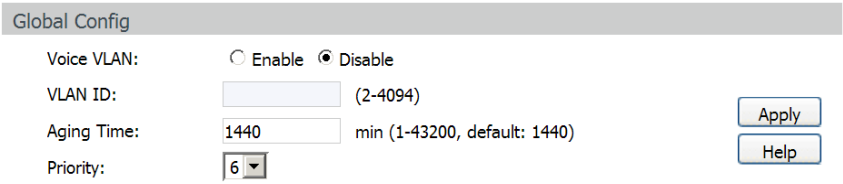
Obs.: *não utilize a VLAN de Voz para transmitir pacotes de dados de outras VLANs, exceto em casos especiais.*

A Voice VLAN pode ser configurada em *Global Config*, *Port Config* e *OUI Config*.

Global config

Nesta página é possível configurar os parâmetros globais da Voice VLAN como por exemplo o VLAN ID, tempo de envelhecimento (Aging Time) e a prioridade de transmissão dos pacotes de voz.

Escolha o menu *QoS → Voice VLAN → Global Config* para carregar a seguinte página:



Configuração de Voice VLAN

As seguintes informações são apresentadas na tela:

» **Global config**

Voice VLAN: selecione *Enable/Disable* para habilitar ou desabilitar a função Voice VLAN

VLAN ID: digite o VLAN ID utilizado pela Voice VLAN.

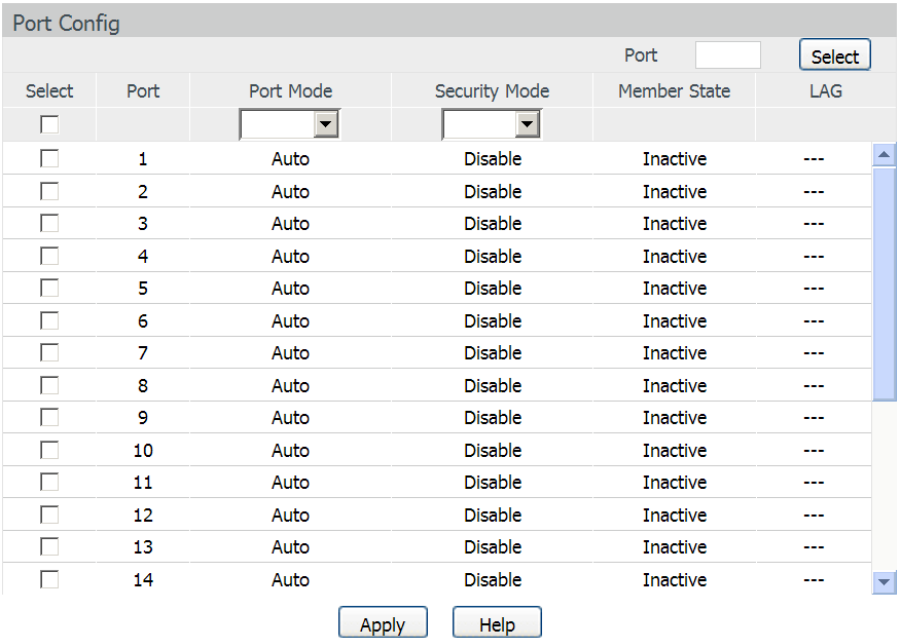
Aging time: especifique o tempo de envelhecimento (aging time) para as portas membro da Voice VLAN que estão no modo automático.

Priority: selecione a prioridade de transmissão dos pacotes de voz na Voice VLAN.

Port config

Nesta página é possível configurar os parâmetros das portas participantes da Voice VLAN.

Escolha o menu *QoS → Voice VLAN → Port Config* para carregar a seguinte página:



Portas da Voice VLAN

Obs.: » *Ao habilitar a função Voice VLAN para um grupo LAG (Agregação da Link), certifique-se que todas as portas do grupo LAG estejam com o mesmo modo de configuração.*

» *Ao modificar o modo de uma porta membro de uma Voice VLAN para automático, fará com que a porta deixe a VLAN de Voz e somente volte quando a porta receber pacotes de voz.*

As seguintes informações são apresentadas na tela:

» **Port config**

Port select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta desejada.

Select: selecione a porta desejada para configurar a Voice VLAN. Neste menu você poderá selecionar um ou mais portas.

Port mode: selecione o modo da porta para se juntar a Voice VLAN.

» Auto: neste modo, o switch adiciona ou remove automaticamente a porta da Voice VLAN, verificando se o tráfego recebido pela porta é de voz ou não.

» Manual: neste modo, é possível adicionar ou remover manualmente uma porta da Voice VLAN.

Security mode: selecione o modo de segurança da porta para o encaminhamento dos pacotes.

» Disable: todos os pacotes serão encaminhados

» Enable: somente pacotes de voz serão encaminhados

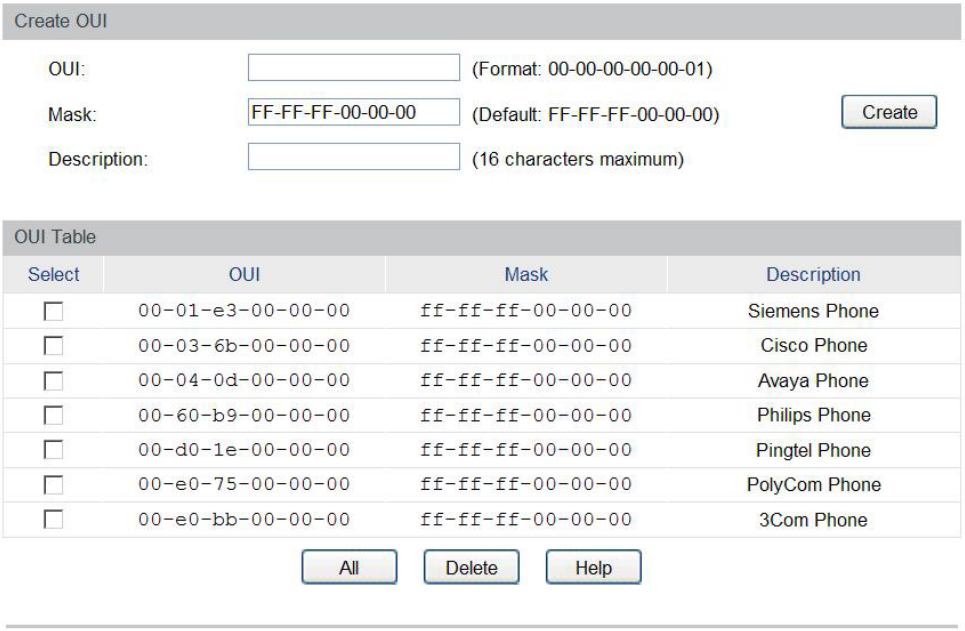
Member state: exibe o estado da porta da Voice VLAN atual.

LAG: exibe o número do grupo LAG a qual a porta pertence.

OUI config

Nesta página é possível adicionar os endereços MAC dos dispositivos de voz, inserindo o endereço OUI do fabricante. O switch determina se um pacote recebido é de voz ou não verificando se o endereço MAC de origem do pacote possui um endereço OUI correspondente, podendo então, adicionar automaticamente a porta para a Voice VLAN.

Escolha no menu *QoS* ⟶ *Voice VLAN* ⟶ *OUI Config* para carregar a seguinte página:



Configuração OUI

» **Create OUI**

OUI: digite o endereço OUI do dispositivo de voz.

MASK: digite a máscara utilizada pelo endereço OUI do dispositivo de voz.

Description: digite uma descrição para identificação do endereço OUI.

» **OUI TABLE**

Select: selecione o endereço OUI desejado. Para remover a entrada, clique no botão *Delete*.

OUI: exibe o endereço OUI do dispositivo de voz.

MASK: exibe a máscara utilizada pelo endereço OUI.

Description: exibe a descrição do endereço OUI.

Procedimentos de configuração da Voice VLAN

Passo	Operação	Descrição
1	Definir o modo de funcionamento das portas	Obrigatório, Em VLAN ⟶ 802.1Q VLAN ⟶ Port Config. Configurar o tipo de link das portas que serão usadas com dispositivos de voz.
2	Criar VLAN	Obrigatório, VLAN ⟶ 802.1Q VLAN ⟶ Port Config. Clique no botão *Create* para criar a VLAN.
3	Adicionar o endereço OUI	Opcional. Em QoS ⟶ Voice VLAN ⟶ OUI Config. Você pode verificar se o switch já tem cadastrado um endereço OUI para seu dispositivo de voz. Caso não possua adicione esse endereço.
4	Configurar os parâmetros de portas para a Voice VLAN	Obrigatório. Em QoS ⟶ Voice VLAN ⟶ Port Config, configure os parâmetros de configuração da porta na Voice VLAN
5	Habilitar a Voice VLAN	Obrigatório. Em QoS ⟶ Voice VLAN ⟶ Global Config, Configure as configurações globais para a Voice VLAN.

10. ACL

ACL (Access Control List) é utilizado para a configuração de regras e políticas para o filtro e processamento dos pacotes, controlando o acesso ilegal a rede. Além disso, a função de ACL pode controlar os fluxos dos dados, economizando recursos da rede de forma flexível, facilitando o controle da rede.

Neste switch, as ACLs classificam os pacotes com base em uma série de condições que podem ser encontrados em protocolos utilizados entre as camadas 2-4 do modelo de referência OSI.

Também é possível controlar as ACLs baseando-se em intervalos de tempo, flexibilizando ainda mais o uso das ACLs.

O menu ACL possui 4 sub-menus de configuração: *Time-Range, ACL Config, Policy Config* e *Policy Binding*.

10.1. Time-Range

Uma ACL baseada em intervalo de tempo permite controlar o tráfego em uma data ou hora específica. Cada regra ACL pode possuir um intervalo de tempo e este intervalo é baseado na data e hora configurado no switch.

Os intervalos de tempo podem ser configurados das seguintes formas:

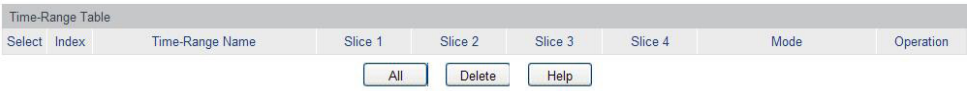
Intervalo de tempo absoluto, intervalo de dias da semana e feriados.

A configuração do intervalo de tempo pode ser configurado no sub-menu *Time Range,* através das seguintes páginas de configuração: *Time-Range Summary, Time-Range* e *Holiday Config*.

Time-Range summary

Nesta página você pode visualizar os time-ranges correntes.

Escolha no menu *ACL → Time Range → Summary* para carregar a seguinte página:



Sumário dos intervalos de tempo

As seguintes informações são exibidas na tela:

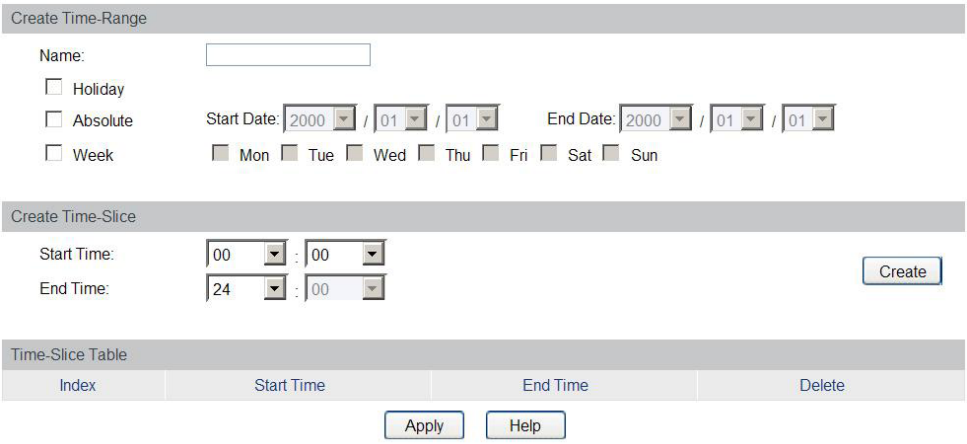
» **Time-Range table**

Select: selecione a entrada desejada para modificar ou remover o Time-Range correspondente.
Index: exibe o índice do Time-Range.
Time-Range Name: exibe o nome do Time-Range
Slice: exibe o Time-Slice (intervalo de tempo) do Time-Range.
Mode: exibe o modo adotado pelo Time-Range.
Operation: clique no botão *Edit* para modificar as configurações do Time-Range desejado ou clique em *Detail* para exibir as informações desse Time-Range.

Time-Range create

Nesta página você pode criar os time-ranges.

Escolha o menu *ACL* → *Time Range* → *Time-Range Create* para carregar a seguinte página:



Configuração do intervalo de tempo

Obs.: *para configurar com êxito o time-range, por favor, em primeiro lugar especifique os time-slices.*

As seguintes opções são apresentadas na tela:

» **Create Time-Range**

Name: digite o nome para o time-range.

Holiday: selecione *Holiday* para configurar o Time-Range conforme feriado previamente configurado no switch. A regra de ACL baseada neste Time-Range terá efeito apenas quando a data/hora do switch estiver dentro do intervalo configurado para o feriado.

Absolute: selecione *Absolute* para configurar o Time-Range em um intervalo de tempo absoluto. A regra de ACL baseada neste time-range terá efeito apenas quando data/hora do switch estiver dentro do intervalo de tempo absoluto configurado.

Week: selecione *Week* para configurar o Time-Range em um intervalo de dias de semana. A regra de ACL baseada neste time-range, terá efeito apenas quando a data/hora do switch estiver dentro da faixa de dias da semana configurado.

» **Create time slice**

Start time: define o tempo de início do Time-Slice.

End time: define o tempo de término do Time-Slice.

» **Time-Slice table**

Index: exibe o índice do Time-Slice.

Start time: exibe o início do tempo do Time-Slice.

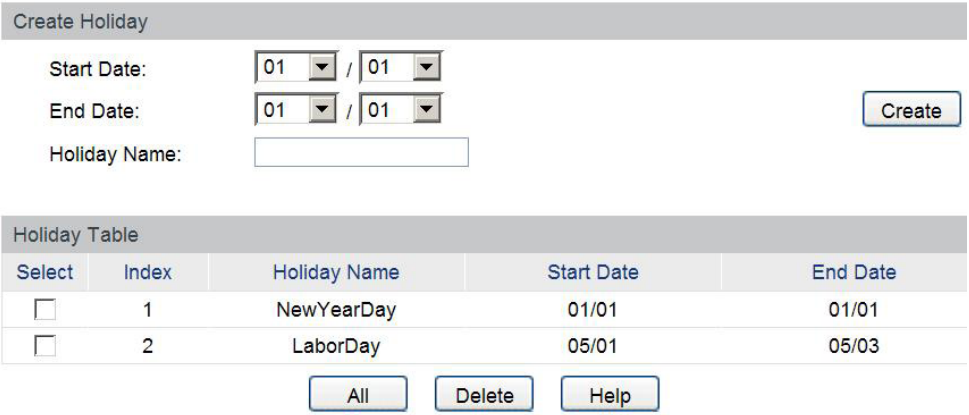
End time: exibe o término do tempo do Time-Slice.

Delete: clique no botão *Delete* para remover o Time-Slice correspondente.

Holiday config

Nesta página é possível configurar os feriados em que regra de ACL será aplicada, conforme sua necessidade.

Escolha no menu *ACL → Time Range → Holiday Config* para carregar a página:



Configuração de feriados As seguintes opções são exibidas na tela:

» **Create holiday**

Start date: selecione a data de início do feriado.
End date: selecione a data de término do feriado.
Holiday name: digite o nome do feriado.

» **Holiday table**

Select: selecione o feriado desejado. Para remover o a entrada criada, clique no botão *Delete*.
Index: exibe o índice do feriado.
Holiday name: exibe o nome do feriado.
Start date: exibe o início do feriado.
End date: exibe o final do feriado.

10.2. ACL config

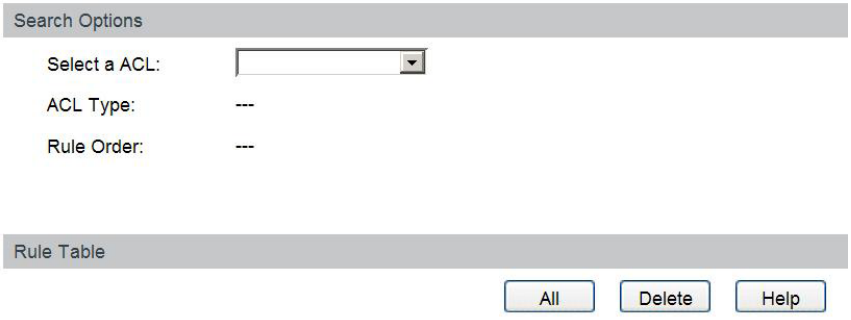
Cada ACL pode conter uma série de regras e cada regra pode especificar um intervalo de tempo diferente. Os pacotes são combinados em ordem. Uma vez que uma regra é correspondida o switch processa os pacotes de acordo com as regras criadas. Sem levar em conta as demais regras, otimizando o desempenho do switch.

As regras ACL podem ser configuradas em: *ACL Summary, ACL Create, MAC ACL, Standard-IP ACL* e *Extend-IP ACL*.

ACL summary

Nesta página você pode visualizar a ACL corrente e configurá-la no switch.

Escolha o menu *ACL* → *ACL Config* → *ACL Summary* para carregar a seguinte página:



ACL

As seguintes informações são apresentadas na tela:

» **Search option**

Select ACL: selecione a ACL desejada.

ACL type: exibe o tipo da ACL selecionada.

Rule order: exibe a ordem das regras de ACL selecionada.

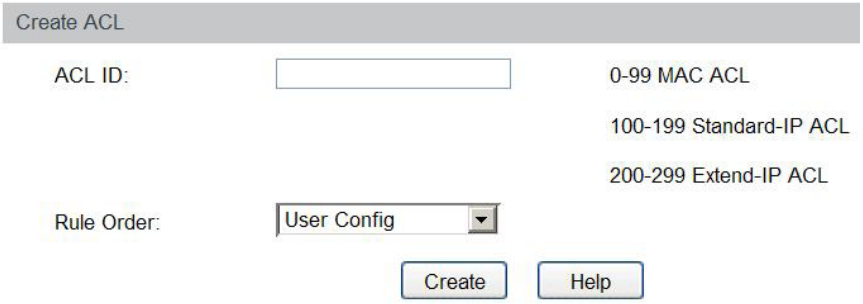
» **Rule table**

Nesta tabela é possível visualizar as informações referentes as regras da ACL selecionada.

ACL create

Nesta página você pode criar ACLs.

Escolha o menu *ACL* → *ACL Config* → *ACL Create* para carregar a seguinte página:



Criação da ACL

As seguintes informações são apresentadas na tela:

» **Create ACL**

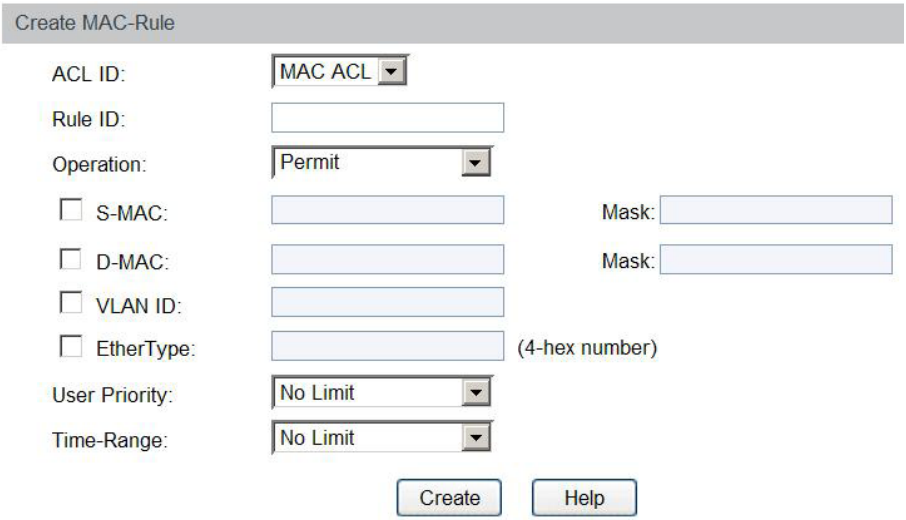
ACL ID: digite o ID da ACL que você deseja criar. O ID é a identificação da ACL, que pode variar de 0 a 299. Existem 3 tipos de ACL que o switch suporta e são identificados pelo número de identificação, *0-99 MAC ACL, 100-199 Standard-IP ACl* e de *200-299 Extend-IP ACL*.

Rule order: User config é a ordem de regras criada pelo usuário e definida para ser a ordem utilizada pela ACL.

MAC ACL

MAC ACLs podem analisar e processar os pacotes com base nas seguintes informações: endereço MAC de origem e destino, VLAN ID e EtherType.

Escolha o menu *ACL* → *ACL Config* → *MAC ACL* para carregar a seguinte página:



MAC ACL

» **Create MAC ACL**

ACL ID: selecione o ID da ACL desejada para realizar a configuração.

Rule ID: digite o ID da regra utilizado pela ACL.

Operation: selecione o modo de operação do switch, quando um pacote corresponder com a regra criada.

» Permit: permite o recebimento do pacote.

» Deny: descarta o pacote recebido.

S-MAC: digite o endereço MAC de origem utilizado pela regra.

D-MAC: digite o endereço MAC de destino utilizado pela regra.

MASK: digite a máscara do endereço MAC.

VLAN ID: digite a VLAN ID utilizada pela regra.

EtherType: digite o EtherType utilizado pela regra.

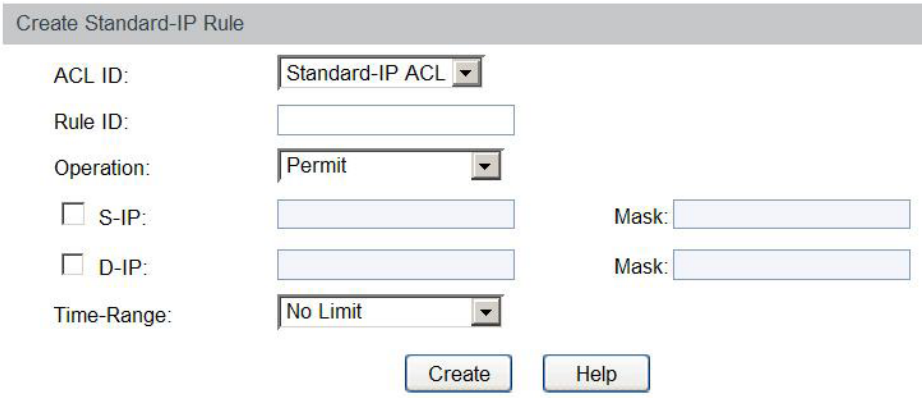
User priority: selecione a prioridade de usuário contida na regra para combinar com os pacotes marcados.

Time range: selecione o Time-Range para que a regra tenha efeito.

Standard-IP ACL

Standard-IP ACLs podem analisar e processar os pacotes com base nas seguintes informações: endereço IP de origem e destino.

Escolha o menu *ACL* → *ACL Config* → *Standard-IP ACL* para carregar a seguinte página:



Standard-IP ACL

As seguintes informações são apresentadas na tela:

» **Create standard-IP ACL**

ACL ID: selecione o ID da ACL desejada para realizar a configuração.

Rule ID: digite o ID da regra utilizado pela ACL

Operation: selecione o modo de operação do switch, quando um pacote corresponder com a regra criada.

» Permit: permite o recebimento do pacote.

» Deny: descarta o pacote recebido.

S-IP: digite o endereço IP de origem utilizado pela regra.

D-IP: digite o endereço IP de destino utilizado pela regra.

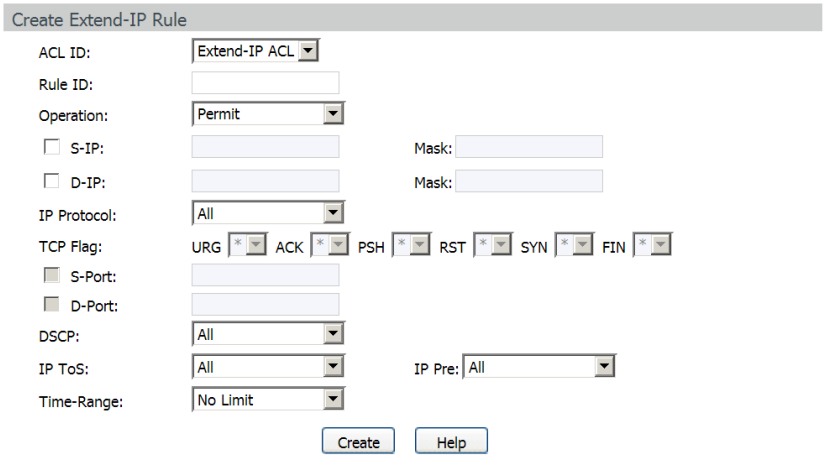
MASK: digite a máscara do endereço IP.

Time-Range: selecione o Time-Range para que a regra tenha efeito.

Extend-IP ACL

Extend-IP ACLs podem analisar e processar os pacotes com base em várias informações, como por exemplo: endereço IP de origem e destino, Flags TCP, portas de origem e destino.

Escolha o menu *ACL → ACL Config → Extend-IP ACL* para carregar a seguinte página:



Extend-IP ACL

As seguintes informações são exibidas na tela:

» **Create extend-IP ACL**

ACL ID: selecione o ID da ACL desejada para realizar a configuração.

Rule ID: digite o ID da regra utilizado pela ACL.

Operation: selecione o modo de operação do switch, quando um pacote corresponder com a regra criada.

» Permit: permite o recebimento do pacote.

» Deny: descarta o pacote recebido.

S-IP: digite o endereço IP de origem utilizado pela regra.

D-IP: digite o endereço IP de destino utilizado pela regra.

MASK: digite a máscara do endereço IP.

IP Protocol: selecione o protocolo de rede utilizado pela regra.

TCP FLAG: configure as flags TCP, quando o protocolo TCP for selecionado na lista.

S-Port: digite a porta de origem utilizada pela regra ACL, quando for selecionado o protocolo de rede TCP ou UDP.

D-Port: digite a porta de destino utilizada pela regra ACL, quando for selecionado o protocolo de rede TCP ou UDP.

DSCP: selecione o valor DSCP contido na regra para ser utilizada pela regra.

IP ToS: selecione o IP-ToS contido na regra.

IP Pre: selecione o IP Precedence contido na regra.

Time-Range: selecione o Time-Range para que a regra tenha efeito.

10.3. Policy config

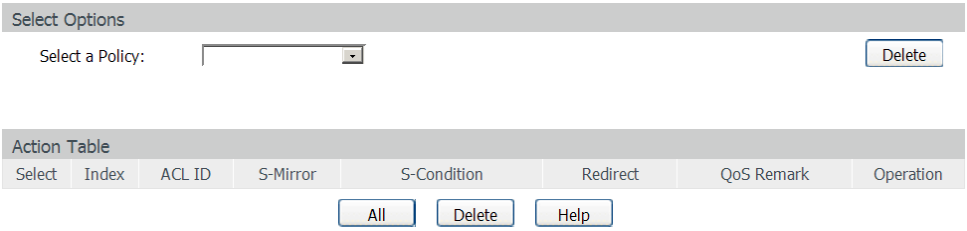
O sub-menu Policy Config é utilizado para controlar os pacotes que cumpram as regras ACLs correspondentes, configurando ações para um conjunto de ACLs. Estas ações incluem Stream Mirror, Stream Condition e Redirect.

A Policy Config pode ser configurada nas seguintes páginas: *Policy Summary, Policy Create* e *Action Create*.

Policy summary

Nesta página é possível visualizar as ações criada na política de ACL para uma determinada regra de ACL.

Escolha o menu *ACL* → *Policy Config* → *Policy Summary* para carregar a página seguinte:



Políticas de ACL

» **Search option**

Select policy: selecione o nome da politica desejada para exibição. Se você desejar excluir uma politica, clique no botão *Delete*.

» **Action table**

Select: selecione a entrada desejada e clique no botão *Edit* para modificar a política criada ou em *Delete* para remover a regra.

Index: exibe o índice da política criada.

ACL ID: exibe o ID da ACL contida na política.

S-Mirror: exibe a porta espelho de origem da política.

S-Condition: exibe a condição de origem acrescentado à política.

Redirect: exibe o redirecionamento adicionado a política.

QoS Remark: exibe a marcação QoS adicionada a política.

Operation: clique no botão *Edit* para modificar política desejada. Após realizado a modificação clique no botão *Submity* para validar a alteração.

Policy create

Nesta página você pode criar as políticas de ACL.

Escolha no menu *ACL → Policy Config → Policy Create* para carregar a seguinte página:

Criação de políticas ACLs

As seguinte opções são exibidas na tela:

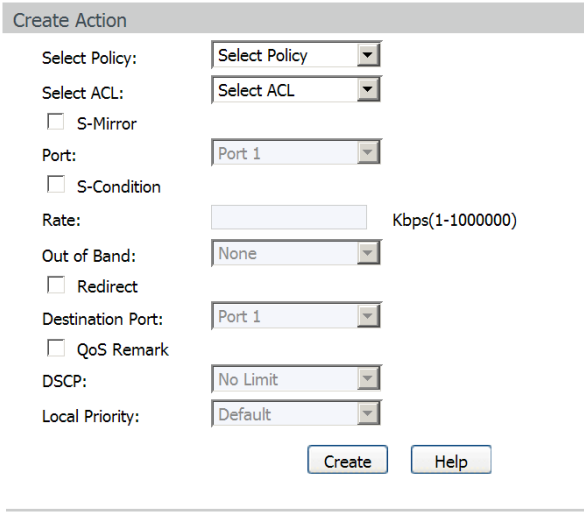
» **Create policy**

Policy name: digite o nome da política ACL.

Action create

Nesta página é possível criar as ações da política de ACL criada, atrelando a política a uma determinada regra de ACL configurada.

Escolha o menu *ACL → Policy Config → Action Create* para carregar a página seguinte:



Ação da política de ACL

As seguintes opções são exibidas na tela:

» **Create action**

Select policy: selecione o nome da política criada.

Select ACL: selecione a regra de ACL que será atrelada a política de ACL.

S-Mirror: selecione *S-Mirror* para espelhar os pacotes de dados na política para uma porta específica.

S-Condition: selecione *S-Condition* para limitar a taxa de transmissão dos pacotes de dados na política.

» Rate: especifique a taxa de transmissão dos pacotes de dados a coincidir com a ACL correspondente.

» Out of Band: especifique se deseja eliminar os pacotes de dados que ultrapassarem o limite da taxa de transmissão especificado no campo *Rate*.

Redirect: selecione *Redirect* para alterar a direção do encaminhamento de pacotes de dados na política.

QoS Remark: selecione remarcação QoS para encaminhar pacotes baseados na configuração de QoS.

» DSCP: selecione a marcação DSCP dos pacotes a coincidir com a ACL desejada.

» Local Priority: selecione a fila de prioridade dos pacotes a coincidir com a ACL desejada.

10.4. Policy binding

A função Policy Binding é utilizada para atrelar a política criada a uma porta do switch ou a uma VLAN especifica, isto é, a política criada somente funcionará após a política ser vinculada a uma destas duas opções: *Port Binding* ou *VLAN Binding*.

Policy Binding pode ser configurada nas seguintes páginas: *Binding Table, Port Binding* e *VLAN Binding*.

Binding table

Nesta página é possível verificar os vínculos criados para as políticas de ACL.

Escolha o menu *ACL → Policy Binding → Binding Table* para carregar a seguinte página:

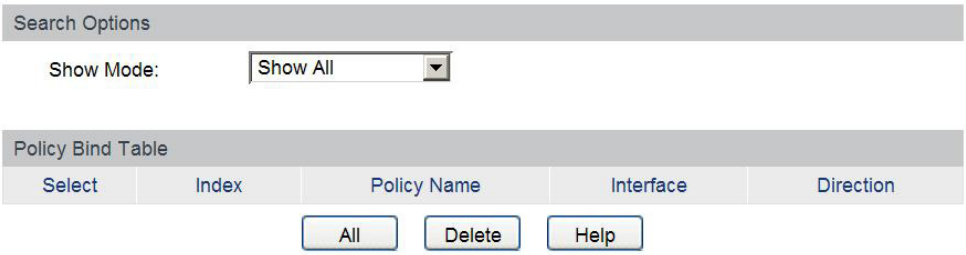


Tabela de vínculos ACL

As seguintes informações são apresentadas na tela:

» **Search option**

Show Mode: selecione o modo do vínculo desejado para visualizar as informações.

» **Policy bind table**

Select: selecione o vínculo desejado e clique em *Delete* para removê-lo da tabela.

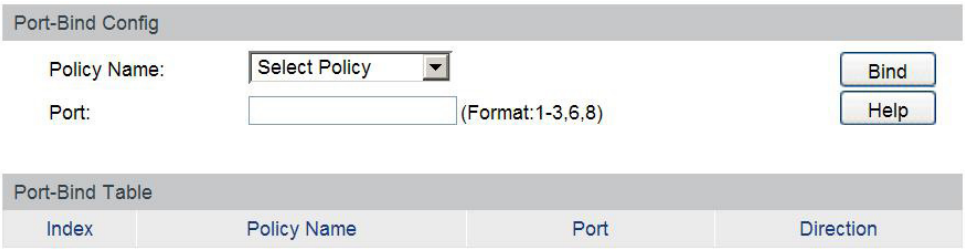
Index: exibe o índice do Binding Policy.

Policy name: exibe o nome do Binding Policy.

Interface: exibe o número da porta do switch ou o VLAN ID vinculados a política criada.

Port binding

Nesta página você pode vincular uma porta do switch a uma política criada.



Vínculo por porta

As seguintes informações são exibidas na tela:

» **Port-Bind config**

Policy name: selecione o nome da política que você deseja vincular.

Port: digite o número da porta que você deseja vincular. Utilize o formato: 1-3,6,8.

» **Port-Bind table**

Index: exibe o índice do Policy Binding.

Policy name: exibe o nome do Policy Binding.

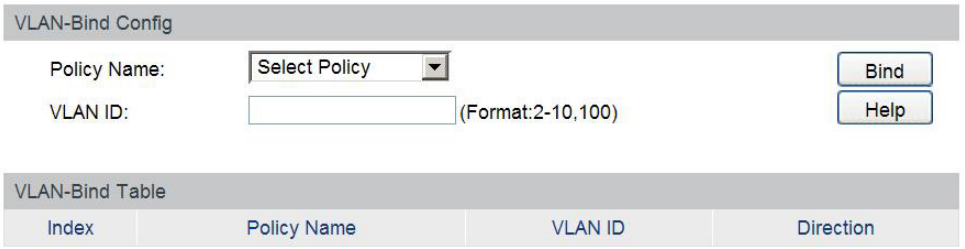
Port: exibe o número da porta do switch vinculado a política correspondente.

Direction: exibe a direção do vínculo.

VLAN binding

Nesta página você pode vincular uma VLAN a uma política criada.

Escolha o menu *ACL → Policy Binding → VLAN Binding* para carregar a seguinte página:



Vínculo por VLAN

As seguintes informações são apresentadas na tela.

» **VLAN-Bind config**

Policy name: selecione o nome da política que você deseja vincular.

VLAN ID: digite o VLAN ID que você deseja vincular. Utilize o formato: 2-10,100.

» **VLAN-Binding table**

Index: exibe o índice do Policy Binding.

Policy name: exibe o nome do Policy Binding.

VLAN ID: exibe o VLAN ID vinculado a política correspondente.

Direction: exibe a direção do vínculo.

Procedimento de configuração

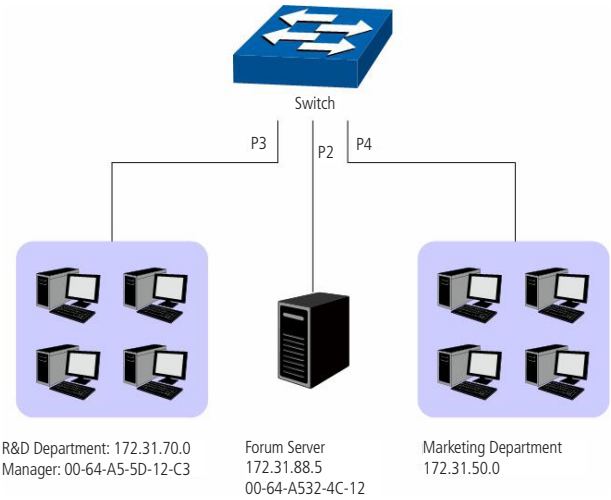
Passo	Operação	Descrição
1	Configuração do time-range efetivo	Obrigatório, ACL ⟶ Time-Range, configure o time-range efetivo para as ACLs.
2	Configuração das regras ACL	Obrigatório, ACL ⟶ ACL Config, configure as regras ACL correspondentes aos pacotes desejados.
3	Configuração de Política ACL	Obrigatório, ACL ⟶ Policy Config, configure as ações das políticas para controlar os pacotes que corresponde às regras ACLs.
4	Vincular uma política a uma porta ou VLAN	Obrigatório, ACL ⟶ Policy Binding, vincular uma porta ou VLAN a uma política criada.

10.5. Exemplos de aplicação para ACL

» **Requerimentos para rede**

1. O gerente do departamento de P&D poderá acessar o fórum da empresa e da internet sem nenhuma restrição. O endereço MAC do gerente é 00-46-A5-5D-12-C3.
2. O pessoal do time de P&D, não poderá acessar a internet durante o horário de trabalho, mas poderão visitar o fórum o dia todo.
3. O pessoal de marketing poderá acessar a internet o dia todo, mas não poderão visitar o fórum durante o horário de trabalho.
4. O departamento de P&D e o departamento de Marketing não poderão se comunicar uns com os outros.

» **Diagrama de rede**



Aplicação de regras ACLs

» **Procedimento de configuração**

Passo	Operação	Descrição
1	Configuração do Time-Range	Em ACL ⟶ Time-Range, crie um nome para o time-range. Selecione o modo Week e configure os dias da semana de segunda a sexta-feira. Adicione o time-slice 08:00 ~ 18:00.
2	Configuração do requerimento 1	ACL ⟶ ACL Config ⟶ ACL Create, crie a ACL 11. ACL ⟶ ACL Config ⟶ MAC ACL, selecione ACL 11, crie a regra 1, configure o campo Operation como Permit, configure o S-MAC como 00-45-A5-5D-12-C3 e a MASK como FF-FF-FF-FF-FF-FF, e configure o time-range como No Limit. ACL ⟶ Policy Config ⟶ Policy Create, crie uma política e nomeie-a para gerente. ACL ⟶ Policy Config ⟶Action Create, adicione na ACL 11 a política gerente. ACL ⟶ Policy Binding ⟶ Port Binding, selecione a política gerente e vincule a porta 3.
3	Configuração dos requerimentos 2 e 4	ACL ⟶ ACL Config ⟶ ACL Create, crie a ACL 100. ACL ⟶ ACL Config ⟶ Standard-IP ACL, Selecione a ACL 100, crie a regra 1, configure o campo Operation como Deny, configure o S-IP como 172.31.70.1 e a máscara como 255.255.255.0, configure o D-IP como 172.31.50.1 e a máscara como 255.255.255.0, configure o time-range como No-Limit. ACL ⟶ ACL Config ⟶ Standard-IP ACL, selecione a ACL 100, crie a regra 2, configure o campo Operation como Deny, configure o S-IP como 172.31.70.1 e a máscara como 255.255.255.0. Configure o D-IP como 172.31.88.5 e a máscara como 255.255.255.0, configure o time-range como No Limit. ACL ⟶ ACL Config ⟶ Standard-IP, Selecione a ACL 100, crie a regra 3, configure o campo Operation como Permit, configure o S-IP como 172.31.70.1 e a máscara como 255.255.255.0, configure o D-IP como 172.31.88.5 e a máscara como 255.255.255.0, configure o Time-Range como work_time. ACL ⟶ Policy Config ⟶ Action Create, adicione a ACL 100 para a política limit 1. ACL ⟶ Policy Binding ⟶ Port Binding, Selecione a política limit 1 para se vincular com a porta 3.
4	Configuração dos requerimentos 3 e 4	ACL ⟶ ACL Config ⟶ ACL Create, crie a ACL 101. ACL ⟶ ACL Config ⟶ Standard-IP ACL, Selecione a ACL 101, crie a regra 1, configure o campo Operation como Deny, configure o S-IP como 172.31.70.1 e a máscara como 255.255.255.0, configure o D-IP como 172.31.50.1 e a máscara como 255.255.255.0, configure o time-range como No-Limit. ACL ⟶ ACL Config ⟶ Standard-IP ACL, selecione a ACL 101, crie a regra 2, configure o campo Operation como Deny, configure o S-IP como 172.31.70.1 e a máscara como 255.255.255.0. Configure o D-IP como 172.31.88.5 e a máscara como 255.255.255.0, configure o time-range como No Limit. ACL ⟶ Policy Config ⟶ Policy Create, crie a política com o nome limit2. ACL ⟶ Policy Config ⟶ Action Create, adicione a ACL 101 para a política limit 1. ACL ⟶ Policy binding ⟶ Port Binding, selecione a política limit2 para se vincular com a porta 4.

11. Network security

O menu Network Security é utilizado para fornecer e configurar várias medidas de proteção para a segurança da rede. Este menu inclui 4 sub-menus: *IP-MAC Binding, ARP Inspection, DoS Defend* e *802.1X*. Por favor, configure as funções conforme sua necessidade.

11.1. IP-MAC binding

A função IP-MAC Binding permite vincular o endereço IP, o endereço MAC e o VLAN ID de um host com uma determinada porta do switch, restringindo o acesso à rede.

Os seguintes métodos de IP-MAC Binding são suportados pelo switch.

1. Manually: você pode vincular o endereço IP, endereço MAC e VLAN ID do host com a porta do switch manualmente.
2. Scanning: você pode vincular o endereço IP, endereço MAC, VLAN ID e a porta em que o host está conectado no switch de forma dinâmica, bastando apenas especificar a faixa de endereços IPs a ser pesquisada bem como o VLAN ID. Após realizado a pesquisa, selecionar quais entradas deseja vincular.
3. DHCP Snooping: você pode utilizar a função de DHCP Snooping para monitorar o processo em que o host recebe o endereço IP de um servidor DHCP e registrar o endereço IP, endereço MAC, VLAN ID e o número da porta em que o host está conectado no switch, realizando assim, um vínculo automático.

Esses três métodos são utilizados para elaboração da tabela de vínculos (Binding Table), vinculando o endereço IP, endereço MAC, VLAN ID e porta do switch onde o host está conectado. As entradas provenientes de várias origens devem ser diferenciadas umas das outras para que se evitem colisões, somente a origem com maior prioridade será validada. Os três métodos (manual, scanning e snooping) estão respectivamente em ordem decrescente de prioridade.

A função IP-MAC Binding pode ser configurada em *Binding Table, Manual Binding, ARP Scanning* e *DHCP Snooping*.

Binding table

Nesta página você pode visualizar as informações referente a tabela de vínculos (Binding Table).

Escolha o menu *Network Security → IP-MAC binding → Binding Table* para carregar a seguinte página:

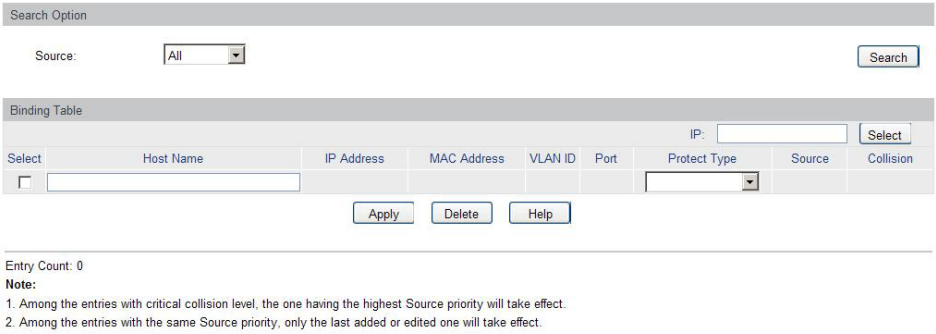


Tabela de vínculos

As seguintes opções são apresentadas na tela:

» **Search option**

Source: selecione o método de busca para a visualização da tabela de vínculos (Binding Table) e clique no botão *Search*.

» All: exibe todas as entradas da tabela.

» Manual: exibe somente as entradas configuradas manualmente.

» Scanning: exibe somente as entradas configuradas a partir da função ARP Scanning.

» Snooping: exibe somente as entradas configuradas a partir da função DHCP Snooping.

» **Binding table**

IP select: digite o endereço IP no campo correspondente e clique em *Select* para selecionar o endereço IP desejado.

Select: selecione a entrada desejada. Nesta opção é possível selecionar mais de uma entrada simultaneamente. Também é possível criar uma descrição para o host utilizando o campo *HostName* e alterar o tipo de proteção através do campo *Protect Type* ou remover a entrada desejada clicando no botão *Delete*.

Host name: exibe o Host Name do computador.

IP address: exibe o endereço IP do computador.

MAC address: exibe o endereço MAC do computador.

VLAN ID: exibe a VLAN ID que o computador pertence.

Port: exibe o número da porta do switch em que o computador está conectado.

Protect type: permite visualizar ou alterar o Protect Type da porta.

Source: exibe o método utilizado para a obtenção da entrada na tabela de vínculos.

Collision: exibe o status de colisão.

» Warning: indica que a colisão pode ter sido causada pela função MSTP.

» Critical: indica que uma entrada está em colisão com outra entrada.

Obs.: *» Dentre as entradas com nível crítico de colisão, aquelas com prioridades mais altas terão preferência.*

» Dentre as entradas conflitantes com o mesmo nível de prioridade, apenas a última entrada adicionada ou modificada terá efeito.

Manual binding

Nesta página você pode vincular manualmente o endereço IP, endereço MAC, e o VLAN ID do host com a porta do switch desejada.

Escolha o menu *Network Security → IP-MAC Binding → Manual Binding* para carregar a página:

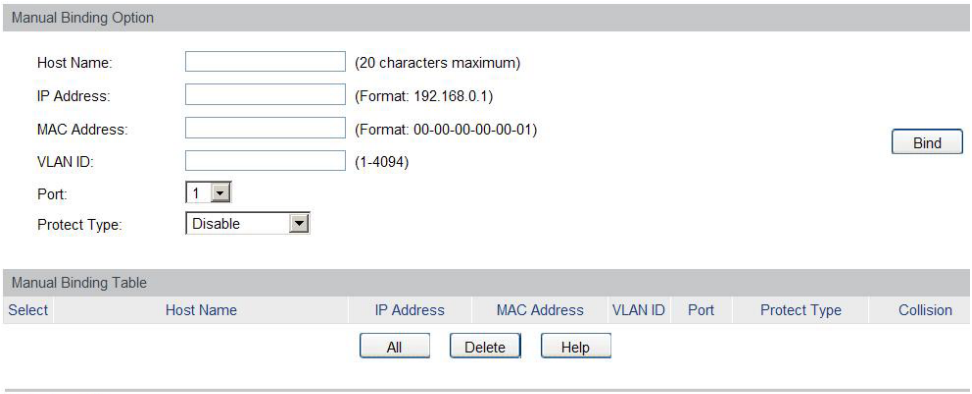


Tabela de vínculos manuais

As seguintes opções são exibidas na tela:

» **Manual binding option**

Host name: digite um nome para identificar o computador desejado.

IP address: digite o endereço IP do computador.

MAC address: digite o endereço MAC do computador.

VLAN ID: digite o VLAN ID que o computador pertence.

Port: selecione a porta do switch em que o computador está conectado.

Protect type: selecione o Protec Type.

» **Manual binding table**

Select: selecione a entrada desejada. Nesta opção é possível selecionar mais de uma entrada simultaneamente. Também é possível criar uma descrição para o host utilizando o campo *HostName* e alterar o tipo de proteção através do campo *Protect Type* ou remover a entrada desejada clicando no botão *Delete*.

Host name: exibe o Host Name do computador.

IP address: exibe o endereço IP do computador.

MAC address: exibe o endereço MAC do computador.

VLAN ID: exibe a VLAN ID que o computador pertence.

Port: exibe o número da porta do switch em que o computador está conectado.

Protect type: exibe o Protect Type.

Collison: exibe o status de colisão.

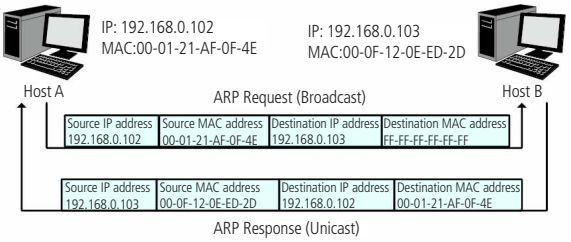
» Warning: indica que a colisão pode ter sido causada pela função MSTP.

» Critical: indica que uma entrada está em colisão com outra entrada.

ARP scanning

O protocolo ARP (Address Resolution Protocol) é utilizado para analisar e mapear os endereços IP com seus respectivos endereços MAC, possibilitando assim a entrega dos pacotes aos seus destinos corretamente. Desta forma, o endereço IP de destino contido em um pacote precisa ser traduzido para o endereço MAC correspondente, formando assim a Tabela ARP.

Quando um computador se comunica com outro, o protocolo ARP funciona conforme imagem e explicação a seguir:



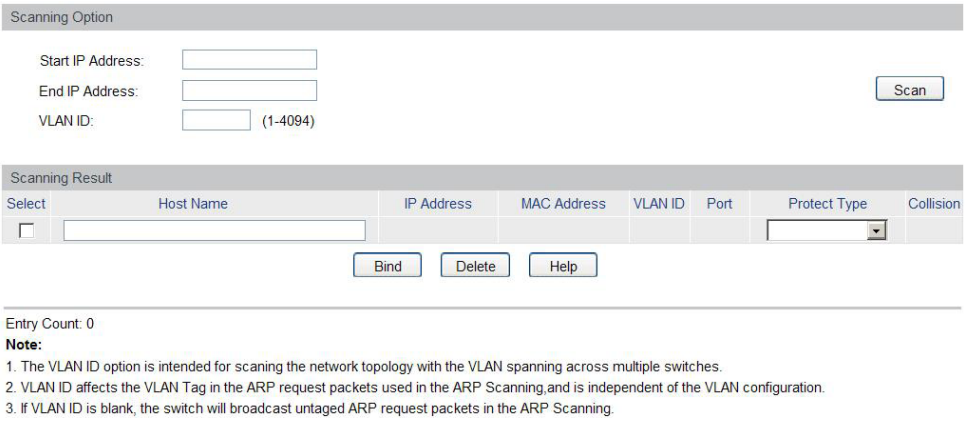
Funcionamento do protocolo ARP

1. Suponha que há dois computadores pertencentes a mesma rede: computador A e o computador B. Para que o computador A possa enviar pacotes para o computador B, o computador A verifica se em sua tabela ARP há o relacionamento entre o endereço IP e o endereço MAC do computador B, caso possua, o pacote será transmitido diretamente ao computador B, caso não possua, o computador A transmitirá solicitações ARP em broadcast para a rede.
2. Quando um pacote de solicitação ARP é transmitido em broadcast, todos os computadores pertencentes a mesma rede visualizarão este pacote, no entanto, apenas o computador B responderá ao pedido, pois o endereço IP contido na solicitação ARP corresponderá com seu próprio endereço IP. Então o computador B enviará ao computador A um pacote de resposta contendo seu endereço MAC.
3. Ao receber o pacote de resposta ARP, o computador A adiciona o endereço IP e o endereço MAC do computador B em sua tabela ARP, para que os próximos pacotes com destino ao computador B sejam encaminhados diretamente ao destino correto.

A função ARP Scanning permite que o switch envie requisições ARP com o campo endereço IP preenchido conforme desejado, dentro de uma rede ou VLAN.

Ao receber pacotes de resposta ARP, o switch consegue, obter o endereço IP, endereço MAC, VLAN ID e o número da porta em que o computador está conectado no switch.

Escolha o menu *Network Security → IP MAC Binding → ARP Scanning* para carregar a seguinte página:


Scanning Option
Start IP Address:
End IP Address:
VLAN ID:
(1-4094)
Scan
Scanning Result
Select
Host Name
IP Address
MAC Address
VLAN ID
Port
Protect Type
Collision
Bind
Delete
Help
Entry Count: 0
Note:
1. The VLAN ID option is intended for scaning the network topology with the VLAN spanning across multiple switches.
2. VLAN ID affects the VLAN Tag in the ARP request packets used in the ARP Scanning,and is independent of the VLAN configuration.
3. If VLAN ID is blank, the switch will broadcast untaged ARP request packets in the ARP Scanning.

ARP Scanning

As seguintes opções são exibidas na tela:

» **Scanning option**

Start IP address: digite o endereço IP inicial da faixa de endereços IPs desejado.

End IP address: digite o endereço IP final da faixa de endereços IPs desejado.

VLAN ID: digite a VLAN ID desejada. Se este campo estiver em branco, o switch irá enviar os pacotes untag para análise.

Scan: clique no botão *Scan* para o switch começar a realizar a consulta desejada.

» **Scanning result**

Select: selecione a entrada desejada. Para remover a entrada correspondente, clique no botão *Delete*.

Host name: exibe o nome do computador.

IP address: exibe o endereço IP do computador.

MAC address: exibe o endereço MAC do computador.

VLAN ID: exibe a VLAN ID que o computador pertence.

Port: exibe o número da porta do switch em que o computador está conectado.

Protect type: exibe o Protect Type.

Collison: exibe o status de colisão.

» Warning: indica que a colisão pode ter sido causada pela função MSTP.

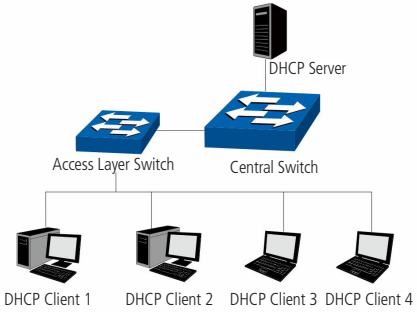
» Critical: indica que um entrada está em colisão com outra entrada.

DHCP snooping

Atualmente as redes estão ficando cada vez maiores e mais complexas. As configurações de endereços IP e parâmetros de redes utilizados devem ser analisados e atualizados com frequência, permitindo o perfeito funcionamento dos computadores e recursos da rede. O protocolo DHCP (Dynamic Host Configuration Protocol) foi desenvolvido baseando-se no protocolo BOOTP e é utilizado para otimizar e resolver os problemas mencionados acima.

» **Principio de funcionamento do Servidor DHCP**

O DHCP funciona baseado na comunicação cliente/servidor. O cliente requisita informações para sua configuração e o servidor atribui as informações de configuração, como por exemplo o endereço IP. Um servidor DHCP pode atribuir endereços IPs para vários clientes, como é ilustrado na figura a seguir:

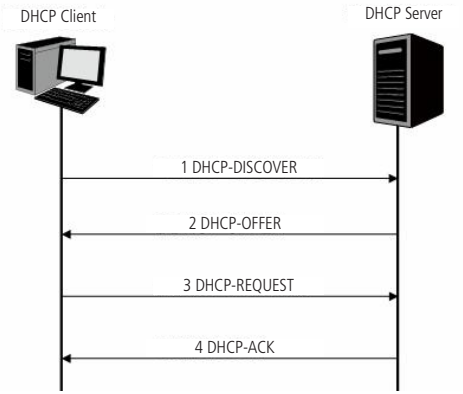


Funcionamento do DHCP

O Servidor DHCP fornece três métodos de atribuição de endereços IPs.

1. Manual: permite o administrador vincular o endereço IP estático para um cliente específico (Ex. Servidor WWW).
2. Automático: o servidor DHCP atribui os endereços IPs para os clientes sem tempo de expiração.
3. Dinâmico: o servidor DHCP atribui o endereço IP com um determinado tempo de expiração. Quando o tempo para o endereço IP expirar, o cliente terá que solicitar um novo endereço IP para o servidor DHCP.

A maioria dos clientes obtêm os endereços IPs dinamicamente, como ilustrado na figura a seguir:



Negociação DHCP

1. **DHCP-DISCOVER:** o cliente transmite em broadcast o pacote DHCP-DISCOVER para descobrir o servidor DHCP.
2. **DHCP-OFFER:** ao receber pacotes DHCP-DISCOVER, o servidor DHCP, escolhe um endereço IP com base em uma faixa com prioridades e responde ao cliente com o pacote DHCP-OFFER contendo o endereço IP e algumas outras informações.
3. **DHCP-REQUEST:** em uma situação em que a vários servidores DHCP enviando pacotes DHCP-OFFER, o cliente só irá responder ao primeiro pacote recebido e transmitir o pacote DHCP-REQUEST, que inclui o endereço IP recebido do pacote DHCP-OFFER.
4. **DHCP-ACK:** uma vez que um pacote DHCP REQUEST é transmitido, todos os servidores DHCP na LAN podem recebê-lo. No entanto, apenas o servidor requisitado processará o pedido. Se o servidor DHCP confirmar a atribuição desse endereço IP para o cliente, ele enviará um pacote DHCP-ACK de volta para o cliente. Caso contrário, o servidor irá enviar pacotes DHCP-NAK, recusando atribuir esse endereço IP para o cliente.

» **Option 82**

Os pacotes DHCP, são classificados de oito maneiras, com base no formato dos pacotes BOOTP. A diferença entre o DHCP e BOOTP é o campo Option. O campo Option do DHCP, é utilizado para expandir a função do DHCP, por exemplo, o DHCP pode transmitir informações de controle e parâmetros da configuração da rede através do campo Option.

Para maiores detalhes do campo Option do DHCP, consulte a RFC 2132.

A opção 82 do campo Option registra a localização dos clientes DHCP. Ao receber um pacote DHCP-REQUEST, o switch adiciona a opção 82 no campo Option no pacote DHCP no pacote e transmite o pacote para o servidor DHCP.

O administrador da rede pode ter o conhecimento da localização do cliente DHCP através do campo Option 82, obtendo maior controle e segurança no gerenciamento dos clientes DHCP. O servidor DHCP que suporta o campo Option 82, pode definir uma política de distribuições dos endereços IPs e outros parâmetros desejados, proporcionando uma distribuição mais flexível dos endereços.

O campo Option 82 pode conter no máximo 255 sub-opções. Uma vez que o campo Option 82 é definido, pelo menos uma das sub-opções deve ser configurada. O switch suporta duas sub-opções: Circuit ID e Remote ID. Como não existe um padrão universal para o campo Option 82, diferentes implementações de diferentes fabricantes podem existir. Para esse switch, as sub-opções são definidas a seguir.

Circuit ID é definido para ser o número da porta do switch que recebe os pacotes de solicitação DHCP juntamente com o VLAN ID.

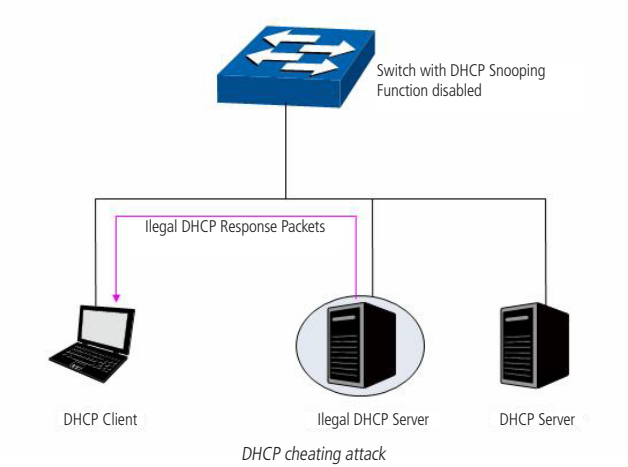
Remote ID é definido para ser o endereço MAC dos clientes DHCP que foram obtidos através dos pacotes DHCP Request.

» **DHCP cheating attack**

Durante o processo de funcionamento do DHCP, geralmente não há nenhum mecanismo de autenticação entre o cliente e servidor. Se houver vários servidores DHCP na rede, acontecerá certa confusão e insegurança na rede. Os casos mais comuns que podem ocorrer estão listados a seguir.

1. O Servidor DHCP ilegal é configurado manualmente pelo usuário por engano.

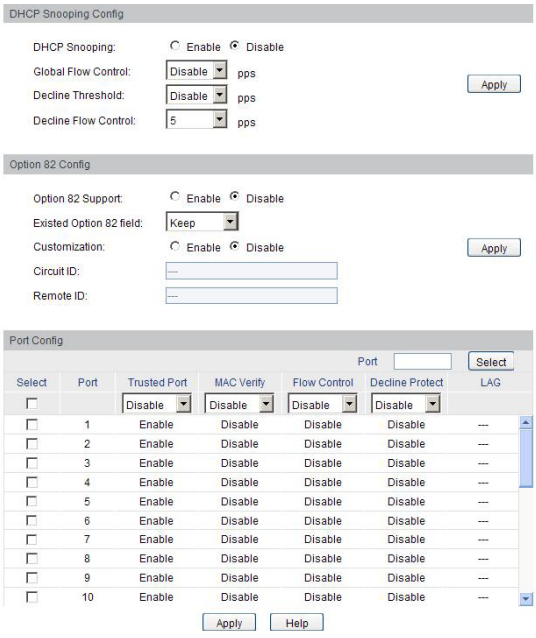
2. Hacker esgotam os endereços IPs do servidor DHCP e fingem ser um servidor DHCP para atribuir os endereços IPs e demais informações de rede para os clientes. Por exemplo. Um Hacker usou o servidor DHCP para atribuir uma modificação no servidor DNS, de modo que os usuários irão acessar sites de comércio eletrônico e digitarão suas senhas achando que esse é o site real. A figura a seguir ilustra a DHCP Cheating Attack.



DHCP cheating attack

A função DHCP Snooping permite que apenas a porta conectada a um servidor DHCP possa transmitir pacotes DHCP, isso garante que os usuários receberam de forma correta os endereços IPs e parâmetros da rede. O DHCP Snooping monitora o processo de obtenção do endereço IP entre o cliente e o servidor DHCP, registrando o endereço IP, endereço MAC, VLAN e porta do swicth que o cliente está conectado, criando assim uma tabela de vínculos, que poderá ser utilizada por outras funções, como por exemplo, ARP Inspection e outros recursos de proteção e segurança. A função de DHCP Snooping impede o DHCP Cheating Attack descartando os pacotes DHCP de portas não confiáveis.

Escolha o menu *Network Security → IP-MAC Binding → DHCP Snooping* para carregar a seguinte página:


DHCP Snooping Config
DHCP Snooping: Enable Disable
Global Flow Control: Disable pps
Decline Threshold: Disable pps
Decline Flow Control: 5 pps
Apply
Option 82 Config
Option 82 Support: Enable Disable
Existed Option 82 field: Keep
Customization: Enable Disable
Circuit ID:
Remote ID:
Apply
Port Config
Port Select
Select Port Trusted Port MAC Verify Flow Control Decline Protect LAG
Disable Disable Disable Disable
1 Enable Disable Disable Disable ---
2 Enable Disable Disable Disable ---
3 Enable Disable Disable Disable ---
4 Enable Disable Disable Disable ---
5 Enable Disable Disable Disable ---
6 Enable Disable Disable Disable ---
7 Enable Disable Disable Disable ---
8 Enable Disable Disable Disable ---
9 Enable Disable Disable Disable ---
10 Enable Disable Disable Disable ---
Apply Help

DHCP snooping

Obs.: *se você quiser habilitar a função de DHCP Snooping para uma porta membro de um grupo LAG, por favor, certifique-se que as configurações das portas membros são as mesmas.*

As seguintes informações são apresentadas na tela:

» **DHCP snooping config**

DHCP snooping: selecione *Enable/Disable* para habilitar ou desabilitar para a função DHCP Snooping.

Global flow control: selecione a velocidade máxima de mensagens DHCP que o switch pode transmitir por segundo. As mensagens excessivas serão descartadas.

Decline threshold: selecione um valor que especifique a taxa mínima de transmissão, acima disso será habilitada a função Decline protection para a porta especificada.

Decline flow control: selecione um valor para especificar o Decline Flow Control. A transmissão de tráfego na porta correspondente será limitada a esse valor.

» **Option 82 config**

Option 82 support: selecione *Enable/Disable* para habilitar ou desabilitar a função Option 82.

Existed option 82 field: selecione a operação para o campo Option 82 dos pacotes de DHCP-REQUEST enviados dos clientes.

» **Keep:** é utilizado para manter o campo Option 82 dos pacotes DHCP.

» **Replace:** é utilizado para substituir o campo Option 82 dos pacotes DHCP com o que foi definido pelo switch.

» **Drop:** é utilizado para descartar os pacotes DHCP incluindo o campo Option 82

Customization: selecione *Enable/Disable* para habilitar ou desabilitar a customização do campo Option 82 pelo switch.

Circuit ID: digite a sub-opção Circuit ID para personalização do campo Option 82.

Remote ID: digite a sub-opção Remote ID para personalização do campo Option 82.

» **Port config**

Port select: digite a porta no campo correspondente e clique em *Select* para selecionar a porta desejada.

Select: selecione a entrada desejada. Nesta opção é possível selecionar mais de uma entrada simultaneamente.

Port: exibe o número da porta.

Trusted port: selecione *Enable/Disable* para habilitar ou desabilitar a função Trusted Port. Somente as Trusted Port podem receber pacotes DHCP dos servidores DHCP.

MAC verify: selecione *Enable/Disable* para habilitar ou desabilitar a função MAC Verity. No pacote DHCP existem dois campos contendo o endereço MAC do cliente, esta função irá comparar estes dois campos e descartar o pacote se os campos forem diferentes.

Flow Control: selecione *Enable/Disable* para habilitar ou desabilitar a função de Flow Control para os pacotes DHCP. Os pacotes DHCP em excesso serão descartados.

Decline protect: selecione *Enable/Disable* para habilitar ou desabilitar a função de Decline Protect.

LAG: exibe o número do grupo LAG a qual a porta pertence.

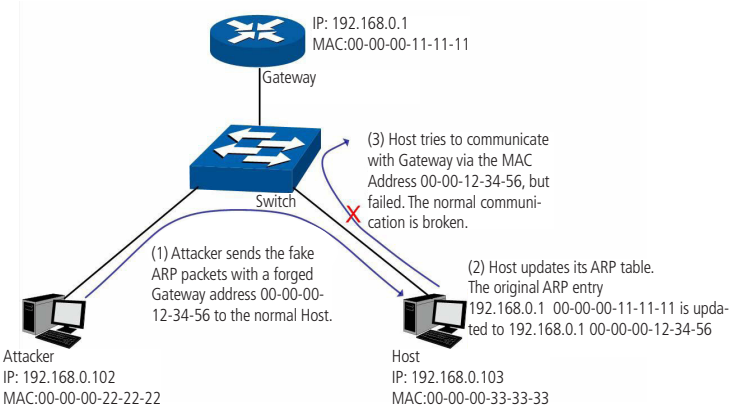
11.2. ARP inspection

De acordo com a implementação ARP, mencionado no Capítulo 11.1.3 ARP Scanning, o protocolo ARP auxilia na comunicação entre os computadores em uma mesma rede ou ainda no acesso a redes externa através do uso do gateway. Assim ataques de falsificação ARP, tais como Imitating Gateway, Cheating Gateway, Cheating Terminal Hosts e ARP Flooding Attack, ocorrem com frequência em redes de grandes dimensões.

A seguir, explicação de alguns dos ataques.

» **Imitating Gateway**

O atacante envia um endereço MAC falso de um gateway para um determinado computador na rede, em seguida este computador atualizará automaticamente a sua tabela ARP, fazendo com que o computador não acesse a rede de forma normal. O imitating Gateway está sendo ilustrado na figura a seguir.

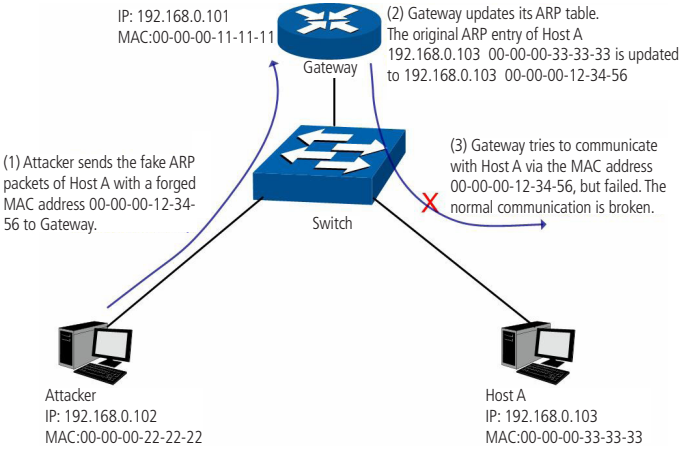

IP: 192.168.0.1
MAC:00-00-00-11-11-11
Gateway
Switch
(3) Host tries to communicate with Gateway via the MAC Address 00-00-12-34-56, but failed. The normal communication is broken.
(1) Attacker sends the fake ARP packets with a forged Gateway address 00-00-00-12-34-56 to the normal Host.
(2) Host updates its ARP table. The original ARP entry 192.168.0.1 00-00-00-11-11-11 is updated to 192.168.0.1 00-00-00-12-34-56
Attacker
IP: 192.168.0.102
MAC:00-00-00-22-22-22
Host
IP: 192.168.0.103
MAC:00-00-00-33-33-33

Imitating Gateway

A figura anterior mostra o atacante enviando pacotes ARP falsificados com o endereço MAC do gateway forjado para um determinado computador na rede, em seguida, este computador atualizará sua tabela ARP automaticamente. Quando o computador tentar se comunicar com outro computador localizado em uma rede externa, ele irá enviar pacotes com o endereço MAC de destino errado, resultando na perda da comunicação.

» **Cheating Gateway**

O atacante envia um endereço MAC falso de um computador para o gateway da rede, em seguida, este gateway atualizará sua tabela ARP, fazendo com que o gateway não consiga responder as solicitações deste computador. O Cheating Gateway é ilustrado na figura a seguir:

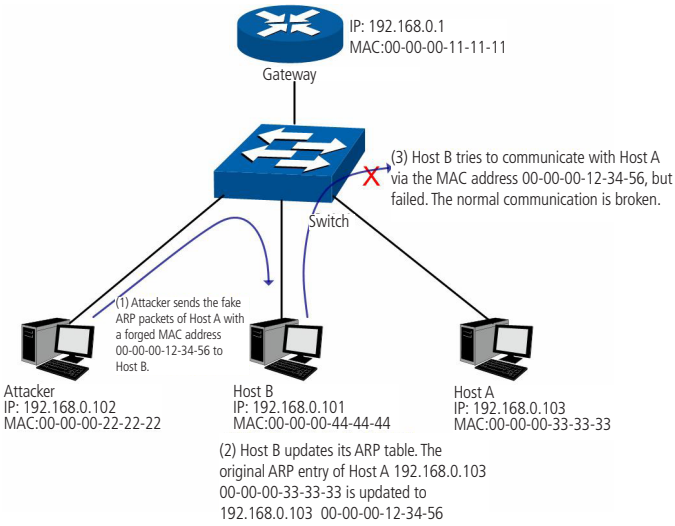

IP: 192.168.0.101
MAC:00-00-00-11-11-11
Gateway
(2) Gateway updates its ARP table. The original ARP entry of Host A 192.168.0.103 00-00-00-33-33-33 is updated to 192.168.0.103 00-00-00-12-34-56
(1) Attacker sends the fake ARP packets of Host A with a forged MAC address 00-00-00-12-34-56 to Gateway.
Switch
(3) Gateway tries to communicate with Host A via the MAC address 00-00-00-12-34-56, but failed. The normal communication is broken.
Attacker
IP: 192.168.0.102
MAC:00-00-00-22-22-22
Host A
IP: 192.168.0.103
MAC:00-00-00-33-33-33

Cheating Gateway

A figura anterior mostra o atacante enviando pacotes ARP falsificados para o gateway da rede, em seguida, este gateway atualizará sua tabela ARP automaticamente. Quando o gateway tentar responder a alguma solicitação do computador correto, o gateway irá enviar pacotes com o endereço MAC de destino errado, resultando na perda da comunicação.

» **Cheating Terminal Host**

O atacante envia um endereço MAC falso de um computador para outro computador da rede, fazendo com que estes computadores que estão na mesma rede não se comuniquem. O Cheating Terminal Hosts é ilustrado na figura a seguir.

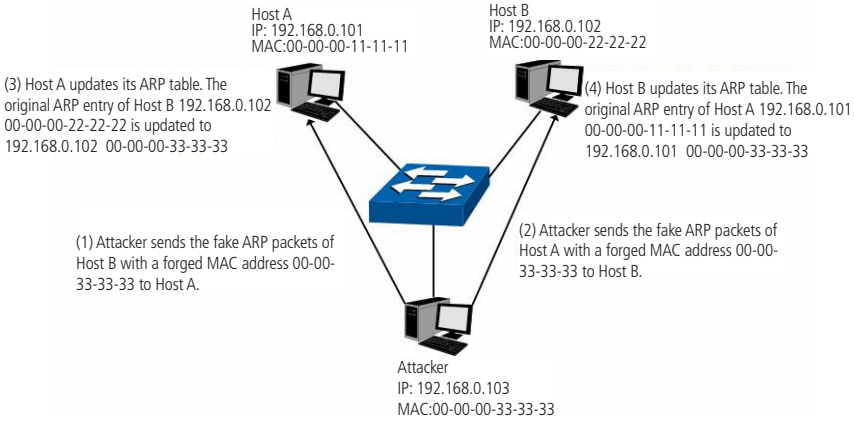

IP: 192.168.0.1
MAC:00-00-00-11-11-11
Gateway
(3) Host B tries to communicate with Host A via the MAC address 00-00-00-12-34-56, but failed. The normal communication is broken.
Switch
(1) Attacker sends the fake ARP packets of Host A with a forged MAC address 00-00-00-12-34-56 to Host B.
Attacker
IP: 192.168.0.102
MAC:00-00-00-22-22-22
Host B
IP: 192.168.0.101
MAC:00-00-00-44-44-44
Host A
IP: 192.168.0.103
MAC:00-00-00-33-33-33
(2) Host B updates its ARP table. The original ARP entry of Host A 192.168.0.103 00-00-00-33-33-33 is updated to 192.168.0.103 00-00-00-12-34-56

Cheating terminal hosts

A figura anterior mostra o atacante enviando pacotes ARP falsificados do computador A para o computador B, fazendo com que a tabela ARP do computador B seja atualizada automaticamente. Quando o computador B tentar se comunicar com o computador A, o computador B enviará pacotes com o endereço MAC de destino errado, resultando na falha da comunicação.

» **Man-In-The-Middle attack**

O Atacante envia continuamente pacotes ARP falsificados para os computadores da rede. Quando estes computadores tentam se comunicar, eles enviarão pacotes para o atacante de acordo com a sua tabela ARP falsificada. Assim o atacante pode obter e processar os pacotes antes de encaminhá-los a seus destino corretos. O Man-In-The-Middle Attack é ilustrado na figura a seguir:


Host A
IP: 192.168.0.101
MAC:00-00-00-11-11-11
Host B
IP: 192.168.0.102
MAC:00-00-00-22-22-22
(3) Host A updates its ARP table. The original ARP entry of Host B 192.168.0.102 00-00-00-22-22-22 is updated to 192.168.0.102 00-00-00-33-33-33
(4) Host B updates its ARP table. The original ARP entry of Host A 192.168.0.101 00-00-00-11-11-11 is updated to 192.168.0.101 00-00-00-33-33-33
(1) Attacker sends the fake ARP packets of Host B with a forged MAC address 00-00-33-33-33 to Host A.
(2) Attacker sends the fake ARP packets of Host A with a forged MAC address 00-00-33-33-33 to Host B.
Attacker
IP: 192.168.0.103
MAC:00-00-00-33-33-33

Man-In-The-Middle attack

Suponha que existam 3 computadores conectados na rede através de um switch.

Computador A: o seu endereço IP é 192.168.0.101 e o endereço MAC é 00-00-00-11-11-11

Computador B: o seu endereço IP é 192.168.0.102 e o endereço MAC é 00-00-00-22-22-22

Atacante: o seu endereço IP é 192.168.0.103 e o endereço MAC é 00-00-00-33-33-33

1. Primeiramente, o atacante envia pacotes de respostas ARP falsificados.
2. Ao receber os pacotes de respostas ARP, os computadores A e B atualizam suas tabelas ARP.
3. Quando o computador A tentar se comunicar com o computador B, ele enviará os pacotes com o endereço MAC de destino falso, ou seja, o endereço MAC de destino do pacote está endereçado para o atacante.
4. Após receber e processar os pacotes dos computadores A e B, o atacante encaminha os pacotes para o endereço MAC correto, fazendo com que os computadores A e B não percebam que suas mensagens estão sendo interceptadas.
5. O atacante continua enviando pacotes ARP falsificados, mantendo a tabela ARP dos computadores A e B erradas.

Na visão dos computadores A e B, os pacotes estão sendo enviados diretamente de um para o outro. Mas na verdade, há um outro computador roubando informações durante o processo de comunicação. Esse tipo de ataque ARP é chamado de Man-In-The-Middle.

» **ARP flooding attack**

O atacante transmite uma quantidade muito grande de pacotes ARP falsificados em um segmento da rede, ocupando muita largura de banda, resultando em uma queda no desempenho da rede. O gateway aprende os endereços IPs/MAC falsificados e atualiza sua tabela ARP, como resultado, a tabela ARP do gateway é totalmente ocupada pelas entradas falsas, tornando-se incapaz de aprender os novos endereços dos computadores verdadeiros, fazendo com que estes não tenham acesso a rede externa.

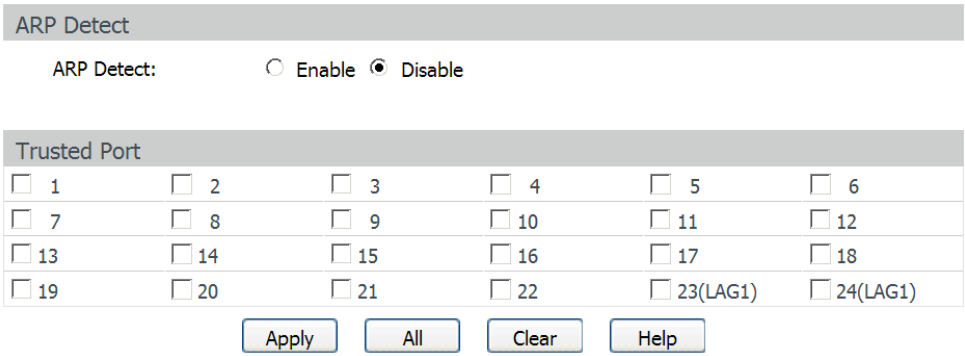
A função IP-MAC Binding permite que o switch possa vincular o endereço IP, endereço MAC, VLAN ID, e o número da porta do switch que o computador está conectado. Com base nos IP-MAC Binding predefinidos, as funções de ARP inspection poderão detectar os pacotes ARP ilegais, evitando assim, ataques ARP na rede.

A função de ARP Inspection pode ser configurada nas seguintes páginas: *ARP Detect, ARP Defend* e *ARP Statistics.*

ARP detect

A função ARP Detect permite ao switch detectar os pacotes ARP com base nas entradas de sua tabela de vínculos (Binding Table) e filtrar os pacotes ARP falsificados, evitando que a rede sofra ataque do tipo ARP, tais como Network Gateway Spoofing e Man-In-The-Middle Attack, etc.

Escolha o menu *Network Security → ARP Inspection → ARP Detect* para carregar a seguinte página:


ARP Detect
ARP Detect: Enable Disable
Trusted Port
1 2 3 4 5 6
7 8 9 10 11 12
13 14 15 16 17 18
19 20 21 22 23(LAG1) 24(LAG1)
Apply All Clear Help
Note:
It's recommended to configure the up-linked port and LAG member as trusted port.

ARP detect

As seguintes opções são exibidas na tela:

» **ARP detect**

ARP detect: selecione *Enable/Disable* para habilitar ou desabilitar a função ARP Detect e clique no botão *Apply*.

» **Trusted port**

Trusted port: selecione a porta que não fará parte do ARP Detect. As portas de up-link e LAG deverão ser definidas como Trusted Port. Para garantir a comunicação normal com o switch, por favor, configure o ARP Trusted Port antes de ativar o ARP Detect.

Obs.: *ARP Detect e ARP Defend não podem ser habilitados ao mesmo tempo.*

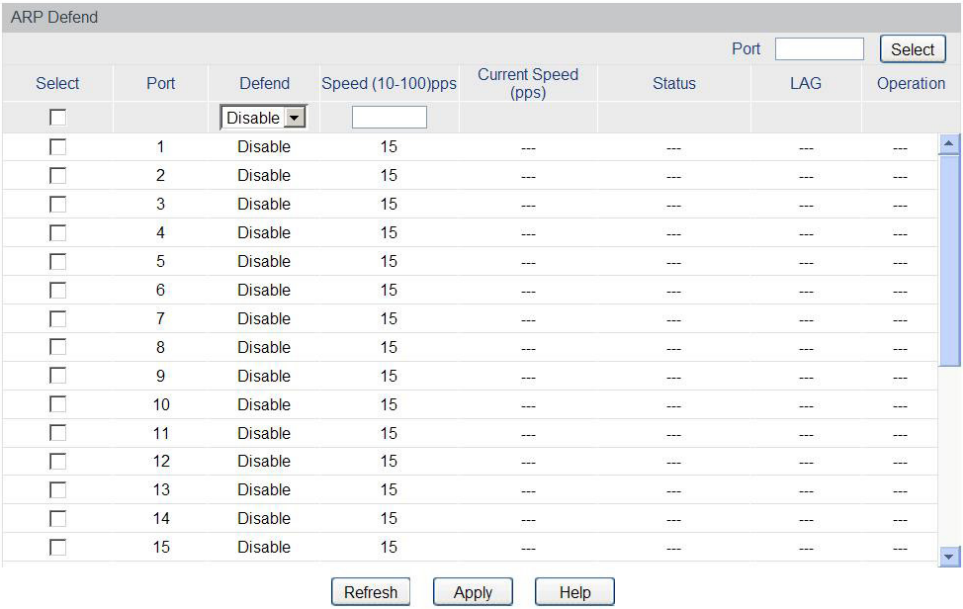
Procedimento de configuração

Passo	Operação	Descrição
1	Vincular o endereço IP, endereço MAC, VLAN ID e o número da porta do switch que o computador está conectado.	Obrigatório, Em IP-MAC Binding, vincular o endereço IP, endereço MAC, VLAN ID e o número da porta do switch que o computador está conectado, através de uma das páginas de configuração: Manual Binding, ARP Scanning ou DHCP Snooping.
2	Habilitar a proteção para a entrada	Obrigatório, Em Network Security ⟶ IP-MAC Binding ⟶ Binding Table, especificar o tipo de proteção para a entrada correspondente.
3	Especificar a Trusted Port	Obrigatório, Em Network Security ⟶ ARP Inspection ⟶ ARP Detect, especificar a Trusted port. As portas up-link e LAG deverão ser definidas como Trusted Port.
4	Habilitar a função ARP Detect	Obrigatório, Em Network Security ⟶ ARP inspection ⟶ ARP Detect, habilite a função ARP Detect.

ARP defend

Com a função ARP Defend habilitada, o switch não recebe pacotes ARP por 300 segundos, quando a velocidade de transmissão de pacotes ARP exceder o valor definido, evitando que ocorra inundação de pacotes ARP na rede.

Escolha o menu *Network Security ⟶ ARP Inspection ⟶ ARP Defend* para carregar a seguinte página:


ARP Defend
Port
Select
Select
Port
Defend
Speed (10-100)pps
Current Speed (pps)
Status
LAG
Operation
Disable
1 Disable 15 --- --- --- ---
2 Disable 15 --- --- --- ---
3 Disable 15 --- --- --- ---
4 Disable 15 --- --- --- ---
5 Disable 15 --- --- --- ---
6 Disable 15 --- --- --- ---
7 Disable 15 --- --- --- ---
8 Disable 15 --- --- --- ---
9 Disable 15 --- --- --- ---
10 Disable 15 --- --- --- ---
11 Disable 15 --- --- --- ---
12 Disable 15 --- --- --- ---
13 Disable 15 --- --- --- ---
14 Disable 15 --- --- --- ---
15 Disable 15 --- --- --- ---
Refresh
Apply
Help
Note:
It is not recommended to enable ARP Defend for LAG member.

ARP defend

As seguintes entradas são exibidas na tela:

» **ARP defend**

Port select: digite a porta deseja no campo correspondente e clique em *Select* para selecionar a porta.

Select: selecione a porta desejada. Nesta opção é possível selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Defend: selecione *Enable/Disable* para habilitar ou desabilitar a função ARP Defend.

Speed: digite o valor para especificar a quantidade máxima de pacotes ARP recebidos por segundo.

Current speed: exibe a velocidade atual dos pacotes ARP recebidos.

Status: exibe o status de ataques ARP.

LAG: exibe o grupo LAG a qual pertence à porta.

Operation: clique no botão *Recover* para restaurar o estado normal da porta. O ARP Defend para essa porta será reativado.

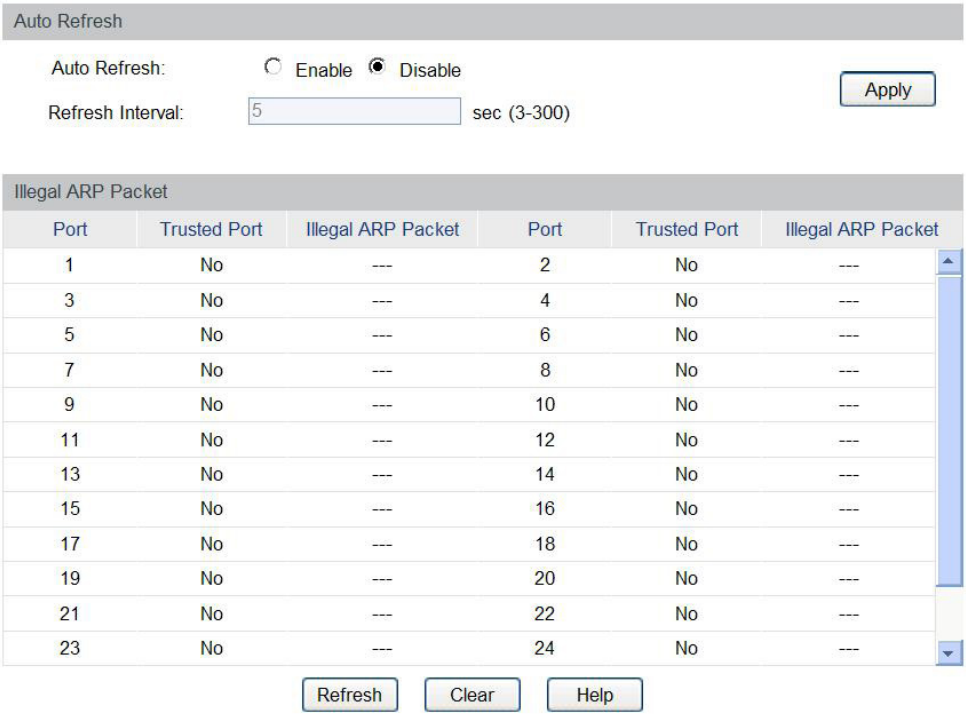
Obs.: *» Não é recomendado habilitar o ARP Defend para portas membros de LAG.*

» As funções ARP Detect e ARP Defend não podem ser habilitadas ao mesmo tempo.

ARP statistics

A função ARP Statistics exibe informações sobre o número de pacotes ARP legítimos recebidos em cada porta, o que facilita a localização de problemas na rede.

Escolha o menu *Network Security* → *ARP Inspection*→ *ARP Statistics* para carregar a página seguinte.


Auto Refresh
Auto Refresh: Enable Disable
Apply
Refresh Interval: 5 sec (3-300)
Illegal ARP Packet
Port Trusted Port Illegal ARP Packet Port Trusted Port Illegal ARP Packet
1 No --- 2 No ---
3 No --- 4 No ---
5 No --- 6 No ---
7 No --- 8 No ---
9 No --- 10 No ---
11 No --- 12 No ---
13 No --- 14 No ---
15 No --- 16 No ---
17 No --- 18 No ---
19 No --- 20 No ---
21 No --- 22 No ---
23 No --- 24 No ---
Refresh
Clear
Help

Estatísticas ARP

As seguintes opções são apresentadas na tela:

» **Auto refresh**

Auto refresh: selecione *Enable/Disable* para habilitar ou desabilitar a função de Auto Refresh.

Refresh interval: digite o intervalo de atualização das estatísticas ARP.

» **Illegal ARP packet**

Port: exibe o número da porta.

Trusted port: indica se a porta está configurada como Trusted Port ou não.

Illegal ARP packet: exibe o número de pacotes ARP falsificados.

11.3. DoS defend

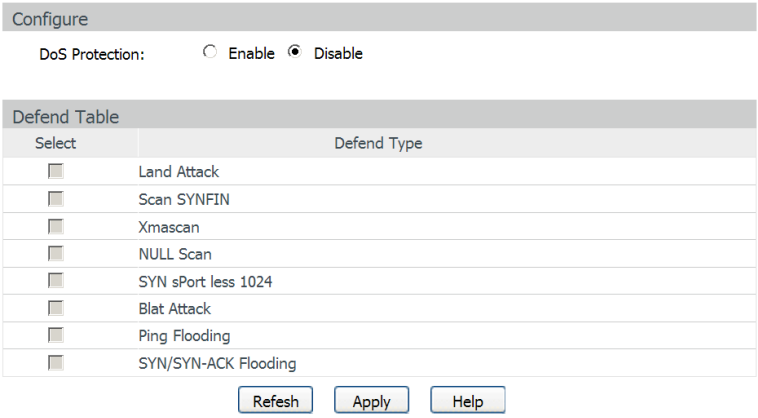
Ataques DoS (Denial of Service) ocasionam lentidão na rede, chegando muitas vezes a parar com o funcionamento do switch, devido a inúmeras requisições maliciosas enviadas pelo atacante. Com esta função habilitada, o switch analisa campos específicos dos pacotes recebidos, podendo permitir ou negar os serviços solicitados, evitando ataques de negação de serviço (DoS).

O switch pode detectar alguns tipos de ataques DoS, conforme mostrado na tabela a seguir.

Tipo de ataque DoS	Descrição
Land Attack	O atacante envia um pacote TCP falso com a flag SYN habilitada para um host de destino. Uma vez que este pacote possua os campos endereço IP de origem e destino configurado de acordo com o endereço IP do host atacado, este host ficará preso em um loop infinito, afetando drasticamente o desempenho da rede.
Scan SYNFIN	O atacante envia um pacote TCP com as flags SYN e FIN habilitadas. A flag SYN é é utilizada para iniciar uma nova conexão, enquanto a flag FIN é utilizada para solicitar uma desconexão. Portanto o pacote deste tipo é ilegal. O switch pode se defender desse tipo de pacote.
Xmascan	O atacante envia o pacote TCP com as seguintes flags habilitadas: FIN, URG e PSH.
NULL Scan Attack	O atacante envia o pacote TCP com todas as flags de controle como 0. Durante a conexão e a transmissão de dados, os pacotes com todos os controles definidos como 0 serão considerados pacotes ilegais.
SYN packet with source port less than 1024	O atacante envia um pacote TCP com a flag SYN habilitada para uma porta de origem menor que 1024.
Blat Attack	O atacante envia um pacote TCP falso com os campos Porta de origem e destino configurados com o mesmo valor e com a flag URG habilitada para um host de destino. Semelhante ao Land Attack, o desempenho do host atacado cairá drasticamente, uma vez que o host sempre tentará iniciar uma nova conexão com o atacante.
Ping Flooding	O atacante faz uma inundação na rede com pings em broadcast, impedindo que o switch responda as verdadeiras comunicações.
SYN/SYN-ACK Flooding	O atacante utiliza um endereço IP falso para enviar pacotes de solicitação ao servidor. Ao receber os pacotes de solicitação, o servidor responde com pacotes SYN-ACK. Como o endereço IP é falso, nenhuma resposta será enviada ao servidor, portanto o servidor continuará enviando pacotes SYN-ACK aguardando uma resposta. Se o atacante ficar enviando muitos pacotes com solicitações falsas, os clientes que realmente desejam utilizar o serviço, terão seus acessos negados.

Nesta página você pode habilitar o DoS Defend adequado para as suas necessidades.

Escolha o menu *Network Security* → *DoS Defend* → *DoS Defend* para carregar a seguinte página:



Ataques DoS

As seguintes opções são apresentadas na tela:

» **Configure**

DoS defend: selecione *Enable/Disable* para habilitar ou desabilitar a função de DoS.

» **Defend table**

Select: selecione o tipo de ataque que o switch irá se defender.

Defend type: exibe o nome do tipo de ataque.

Obs.: » *Sugerimos que você tome as seguintes medidas para garantir a segurança da rede.*

» *É recomendado inspecionar e reparar vulnerabilidades na rede regularmente, bem como adotar métodos de backup das configurações importantes.*

» *O administrador de rede deve inspecionar o ambiente físico e bloquear serviços desnecessários.*

» *Para uma melhor segurança, utilize firewall na rede.*

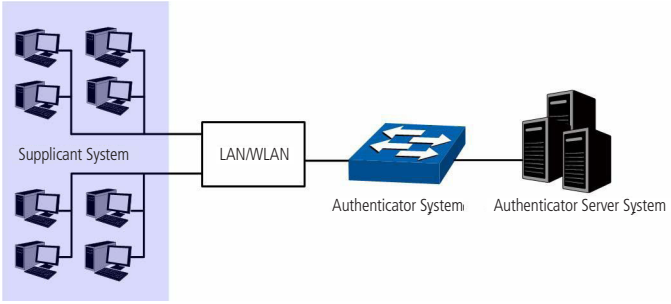
11.4. 802.1X

O protocolo 802.1X foi desenvolvido pela IEEE802 comissão LAN/WAN, para lidar com as questões de segurança de redes sem fio. Em seguida foi utilizado como mecanismo de controle de acesso utilizado pelo Ethernet, resolvendo problemas de autenticação e segurança.

802.1X é o padrão de autenticação para o controle de acesso a rede, onde cada dispositivo da LAN (suplicante) somente irá utilizar a rede se estiver autenticado em um servidor de modo seguro.

» **Arquitetura de autenticação 802.1X**

802.1X adota uma arquitetura de Cliente/Servidor com três entidades: um sistema suplicante, um sistema autenticador e um servidor de autenticação, a figura a seguir ilustra esse processo.



Arquitetura 802.1X

1. Supplicant System: o sistema suplicante é uma entidade da LAN e é autenticado pelo sistema autenticador. O sistema suplicante geralmente é o computador de um usuário da rede. Uma autenticação 802.1X é iniciada quando um usuário lança um programa cliente no sistema suplicante. Note que o programa cliente deve suportar a autenticação 802.1X.
2. Authenticator System: o sistema autenticador geralmente é um dispositivo de rede como esse switch. Ele fornece a porta física ou lógica para o suplicante acessar a LAN e se autenticar.
3. Authentication Server System: o servidor de autenticação é normalmente a entidade que prove o serviço de autenticação. Normalmente é formado por um servidor RADIUS. O servidor de autenticação pode armazenar informações de usuários e serve para realizar autenticação e autorização. Para garantir um sistema de autenticação estável, é recomendado possuir um servidor de autenticação alternativo, utilizado como backup.

» **Mecanismos de autenticação 802.1X**

O sistema de autenticação IEEE802.1X utiliza o protocolo EAP (Extensible Authentication Protocol) para trocar informações entre o sistema suplicante e o servidor de autenticação.

1. O protocolo EAP transmitido entre o sistema suplicante e o sistema autenticador são encapsulados como pacotes EAPOL.
2. O protocolo EAP, transmitido entre o sistema autenticador e o servidor RADIUS são encapsulados como EAPOR (EAP over RADIUS) ou através de PAP (Password Authentication Protocol) ou CHAP (Challenge Handshake Authentication Protocol).

3. Quando um sistema suplicante é processado pelo servidor de autenticação, o servidor de autenticação passa a informação sobre o sistema suplicante para o sistema autenticador. O sistema autenticador, por sua vez determina o estado (autorizado ou não autorizado) da porta de acordo com as instruções (accept ou reject) recebidos do servidor Radius.

» **Procedimento de autenticação 802.1X**

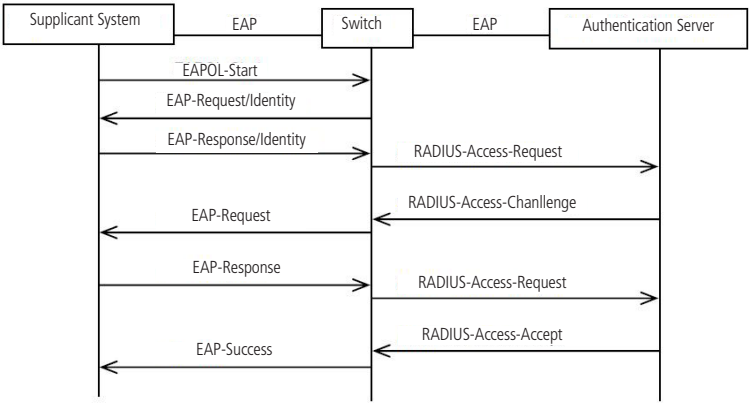
Uma autenticação 802.1X pode ser iniciada pelo sistema suplicante ou pelo sistema autenticador.

Quando um sistema autenticador (switch) detecta um suplicante não autenticado e conectado em sua porta, ele irá iniciar o procedimento de autenticação 802.1X enviando pacotes EAP-Request/Identity. O sistema suplicante também pode iniciar o procedimento de autenticação 802.1X, iniciando um programa cliente de autenticação 802.1X, através do envio de pacotes EAPOL-Start para o switch.

A seguir duas ilustrações de autenticação 802.1X iniciada pelo sistema suplicante.

1. Modo de transmissão EAP:

Neste modo, os pacotes EAP são encapsulados no protocolo de nível superior (EAPOR) para conseguir chegar ao servidor de autenticação. Este modo normalmente exige que o servidor Radius tenha suporte aos dois tipos de mensagens. O campo mensagem EAP e o campo Message-authenticator. Esse switch suporta a forma de autenticação EAP-MD5 para o modo de transmissão EAP. A figura a seguir descreve o procedimento básico de autenticação EAP-MD5.



Procedimento de autenticação EAP-MD5

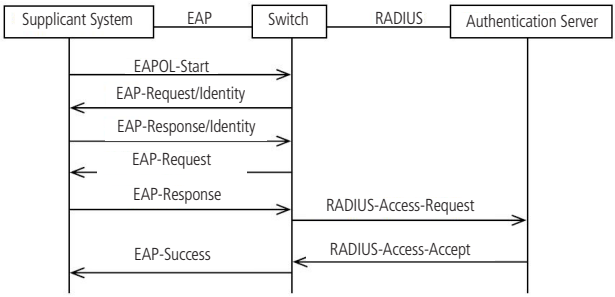
1. Um sistema suplicante inicia um programa cliente de autenticação 802.1X, através de seu nome de usuário e senha cadastrados no servidor de autenticação, enviando um pacote EAPOL-Start para o switch. O programa cliente 802.1X encaminha os pacotes para o switch iniciar o processo de autenticação.
2. Ao receber o pacote de solicitação de autenticação, o switch envia um pacote EAP-Request/Identity para solicitar ao programa cliente 802.1X o nome de seu usuário.
3. O programa 802.1X cliente envia um pacote EAP-Response/Identity para o switch com o nome de usuário. O switch então encapsula o pacote em um pacote RADIUS Access-Request e encaminha o pacote para o servidor RADIUS.
4. Ao receber o nome de usuário do switch, o servidor RADIUS verifica a senha correspondente do usuário em seu banco de dados e criptografa a senha utilizando uma chave aleatória, e encaminha esta chave ao switch através do pacote RADIUS Access-Challenge. O switch em seguida, envia a chave para o programa 802.1X cliente.
5. O receber a chave (encapsulada no pacote EAP-Request/MD5 Challenge) do switch, o programa 802.1X cliente criptografa a senha do sistema suplicante com a chave recebida e envia a senha criptografada (contida no pacote EAP--Response/MD5 Challenge) para o servidor RADIUS através do switch (a criptografia é irreversível).
6. O servidor RADIUS compara a senha criptografada recebida (contida no pacote RADIUS Access-Request) com a senha criptografada localmente. Se as duas combinarem, ele enviará a resposta (através de um pacote RADIUS Access-Accept e do pacote EAP-Success), informando ao switch que o sistema suplicante está autorizado.
7. O switch muda o estado da porta correspondente ao estado accept para permitir que o sistema suplicante tenha acesso à rede. Então o switch irá monitorar o status do suplicante enviando pacotes hand-shake periodicamente. Por padrão, o switch vai forçar o suplicante fazer logoff se não obter a resposta do suplicante em duas tentativas.

8. O sistema suplicante também pode encerrar o estado de autenticação, enviando pacotes EAPOL-Logoff para o switch. O switch então muda o estado da porta para reject.

2. Modo de terminação EAP:

Neste modo, a transmissão de pacotes é encerrada no sistema autenticador e os pacotes EAP são mapeados em pacotes RADIUS. Autenticação e contabilidade são realizadas através de protocolos RADIUS.

Neste modo, o método de autenticação PAP ou CHAP é utilizado entre o switch e o servidor RADIUS. Este switch suporta o modo de encerramento PAP. O procedimento de autenticação PAP é ilustrado na figura a seguir.



Procedimento de autenticação PAP

No modo PAP, o switch criptografa a senha com uma chave gerada aleatoriamente e envia o nome do usuário ao sistema suplicante, o sistema suplicante criptografa a senha para o servidor RADIUS, utilizado para uma autenticação adicional.

Considerando que a chave gerada aleatoriamente no modo de transmissão EAP-MD5 é realizada pelo servidor de autenticação, o switch é o responsável por encapsular o pacote de autenticação e enviá-lo para o servidor RADIUS.

» **802.1X timer**

Na autenticação 802.1X, os seguintes temporizadores são utilizados para assegurar que o sistema suplicante, o switch e o servidor RADIUS interagem de uma maneira ordenada.

1. Supplicant system timer (Supplicant Timeout): este temporizador é acionado pelo switch após o switch enviar um pacote de solicitação ao sistema suplicante. O switch irá reenviar o pacote de solicitação ao sistema suplicante se o sistema suplicante não responder no período de tempo limite especificado.
2. RADIUS server timer (Server Timeout): este temporizador é acionado pelo switch após o switch enviar um pacote de solicitação de autenticação para o servidor RADIUS. O switch irá reenviar o pacote de solicitação de autenticação se o servidor RADIUS não responder no período de tempo limite especificado.
3. Quiet-period timer (Quiet Period): este temporizador define o período de silêncio. Enquanto o sistema suplicante não processa a autenticação, o switch fica em silêncio (não envia pacotes 802.1X) por um período especificado antes de processar outra solicitação de autenticação.

» **Guest VLAN**

A função Guest VLAN permite que os suplicantes que não passam na autenticação possam acessar os recursos de uma rede específica. Por padrão, todas as portas conectadas aos suplicantes pertencem a uma VLAN, ou seja, a Guest VLAN. Usuários pertencentes à Guest VLAN podem acessar os recursos da Guest VLAN sem estarem autenticados. Ao realizar uma autenticação, as portas do switch irão ser removidas da Guest VLAN, permitindo o acesso aos recursos da rede.

Com a função Guest VLAN habilitada, os usuários podem acessar a Guest VLAN para instalar o programa 802.1X cliente ou atualizar seus clientes 802.1X sem estar autenticado. Se não houver suplicantes na porta por certo período de tempo, o switch irá adicionar a porta para a Guest VLAN.

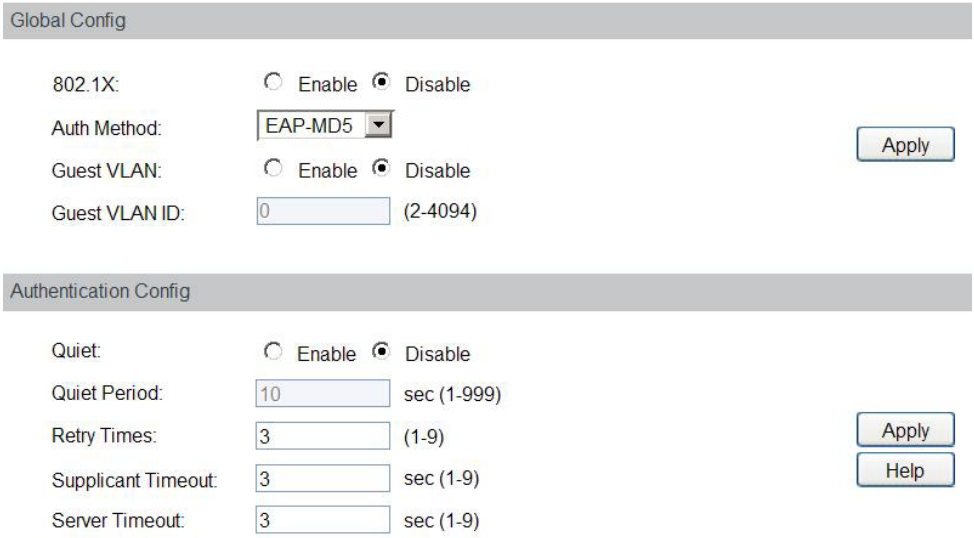
Com a função de 802.1X habilitada e a Guest VLAN configurada, após o número máximo de tentativas terem sido feitas para enviar pacotes EAP-Request/Identity e ainda houver portas que não enviaram nenhuma resposta de volta, o switch irá adicionar essas portas para a Guest VLAN de acordo com seus tipos de Links. Só quando o usuário correspondente realizar a autenticação 802.1X, a porta será removida da Guest VLAN e adicionada a VLAN especificada. Além disso, a porta voltará para a Guest VLAN quando seus usuários conectados fazerem Logoff.

A função 802.1X pode ser configurada nas seguintes páginas: *Global Config, Port Config* e *Radius Server.*

Global config

Nesta página você pode habilitar a função de autenticação 802.1X para controlar o processo de autenticação, especificando o método de autenticação, Guest VLAN e diferentes temporizadores.

Escolha o menu *Network Security → 802.1X → Global Config* para carregar a seguinte página:



Habilitando a autenticação Radius

As seguintes informações são apresentadas na tela:

» **Global config**

802.1X: selecione *Enable/Disable* para habilitar ou desabilitar a função 802.1X

Authentication method: selecione o método de autenticação.

» EAP-MD5: este método de autenticação utiliza o protocolo Extensible Authentication Protocol (EAP) para trocar informações entre o switch e o cliente. Estes pacotes EAP transportam dados de autenticação e podem ser encapsulados por um outro protocolo, como o RADIUS para serem transmitidos para o servidor de autenticação.

» PAP: este método de autenticação utiliza o protocolo Extensible Authentication Protocol (EAP) para trocar informações entre o switch e o cliente. A transmissão dos pacotes EAP é finalizada pelo switch e os Pacotes EAP são convertidos para o outro protocolo (por exemplo, RADIUS) para a transmissão de pacotes.

Guest VLAN: selecione *Enable/Disable* para habilitar ou desabilitar a função Guest VLAN.

Guest VLAN ID: digite o ID desejado para a Guest VLAN. Os suplicantes na Guest VLAN podem acessar recursos da rede específica.

» **Authentication config**

Quiet: selecione *Enable/Disable* para habilitar ou desabilitar o tempo de silêncio.

Quiet period: digite um valor para o período de silêncio, uma vez que o suplicante falhar ao tentar se autenticar via 802.1X, o switch não irá responder a mais pedidos do suplicante em um determinado período de tempo.

Retry times: específica os tempos máximos de transferência para o pedido de autenticações repetidas.

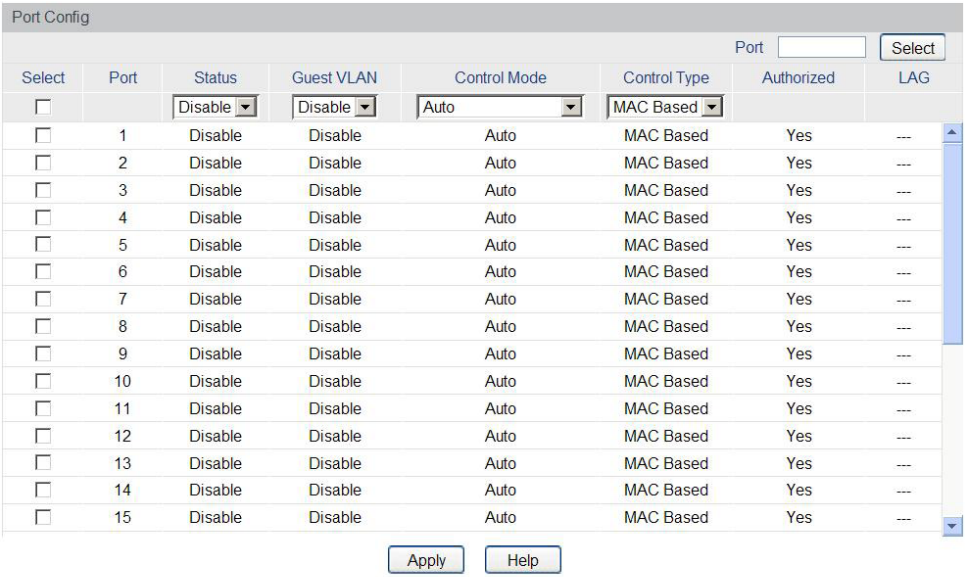
Supplicant timeout: digite o tempo máximo para o switch esperar pela resposta do suplicante antes de reenviar o pacote de solicitação ao suplicante.

Server timeout: digite o tempo máximo para o switch esperar pela resposta do servidor de autenticação antes de reenviar o pacote de solicitação ao servidor de autenticação.

Port config

Nesta página você pode configurar os recursos de autenticação 802.1X para as portas com base nas suas necessidades.

Escolha o menu *Network Security → 802.1X → Port Config* para carregar a seguinte página.


Port Config
Port
Select
Select
Port
Status
Guest VLAN
Control Mode
Control Type
Authorized
LAG
Disable
Disable
Auto
MAC Based
1 Disable Disable Auto MAC Based Yes ---
2 Disable Disable Auto MAC Based Yes ---
3 Disable Disable Auto MAC Based Yes ---
4 Disable Disable Auto MAC Based Yes ---
5 Disable Disable Auto MAC Based Yes ---
6 Disable Disable Auto MAC Based Yes ---
7 Disable Disable Auto MAC Based Yes ---
8 Disable Disable Auto MAC Based Yes ---
9 Disable Disable Auto MAC Based Yes ---
10 Disable Disable Auto MAC Based Yes ---
11 Disable Disable Auto MAC Based Yes ---
12 Disable Disable Auto MAC Based Yes ---
13 Disable Disable Auto MAC Based Yes ---
14 Disable Disable Auto MAC Based Yes ---
15 Disable Disable Auto MAC Based Yes ---
Apply
Help
Note:
802.1X can not be enabled for LAG member.

Configuração Radius

As seguintes informações são apresentadas na tela:

» **Port config**

Port select: digite a porta desejada no campo correspondente e clique em *Select* para selecionar a porta desejada.

Select: selecione a porta desejada. Neste menu você poderá selecionar mais de uma porta simultaneamente.

Port: exibe o número da porta.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a função 802.1X na porta desejada.

Guest VLAN: selecione *Enable/Disable* para habilitar ou desabilitar a função Guest VLAN na porta desejada.

Control mode: selecione o modo de funcionamento da porta desejada.

» Auto: neste modo, a porta irá operar normalmente após a realização da autenticação 802.1X.

» Force-Authorized: neste modo a porta irá operar normalmente sem a realização da autenticação 802.1X.

» Force-Unauthorized: neste modo a porta estará inoperante e não participará do processo de autenticação 802.1X.

Control type: selecione o tipo de controle da porta desejada.

» MAC Based: qualquer cliente conectado na porta deverá passar pela autenticação 802.1X para ter acesso na rede.

» Port Based: todos os clientes conectados na porta podem acessar a rede, com a condição de que qualquer um dos clientes tenha passado na autenticação 802.1X.

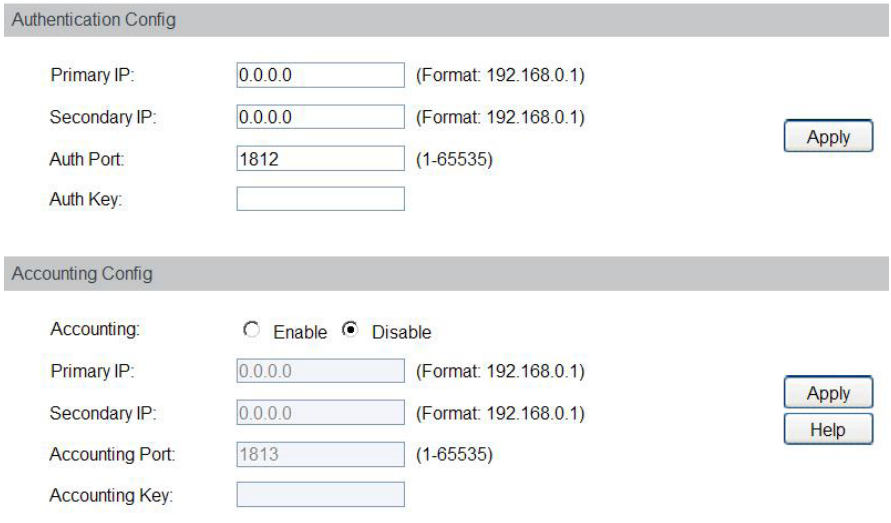
Authorized: exibe o status de autenticação da porta.

LAG: exibe o número do grupo LAG a qual a porta pertence.

Radius Server

Servidor RADIUS (Remote Authentication Dial-In User Service) fornece serviço de autenticação para o switch através de informações de clientes armazenadas, tais como o nome de usuário, senha, etc. Com a finalidade de controlar o estado de autenticação e contabilizar os clientes. Nesta página você pode configurar os parâmetros do servidor de autenticação.

Escolha o menu *Network Security → 802.1X → Radius Server* para carregar a seguinte página.



Configuração do servidor Radius

As seguintes informações são exibidas na tela:

» **Authentication config**

Primary IP: digite o endereço IP do servidor de autenticação.

Secondary IP: digite o endereço IP do servidor de autenticação alternativo.

Authentication port: defina a porta UDP utilizada para a autenticação. Por padrão a porta é 1812.

Authentication KEY: digite a senha configurada no servidor de autenticação, para a realização da troca de mensagens.

» **Accounting config**

Accounting: selecione *Enable/Disable* para habilitar ou desabilitar a função de contabilização.

Primary IP: digite o endereço do servidor IP de contabilidade.

Secondary IP: digite com o endereço IP do servidor de contabilidade alternativo.

Accounting port: defina a porta UDP utilizada para a contabilização. Por padrão a porta é 1812.

Accounting KEY: digite a senha configurada no servidor de contabilização, para a realização da troca de mensagens.

Obs.: *» A função de 802.1X somente terá efeito quando for habilitada globalmente no switch e também nas portas participantes.*

» A função 802.1X não poderá ser habilitada para portas membros de um grupo LAG.

» A função 802.1X não deve ser habilitada na porta conectada ao servidor de autenticação. Além disso, os parâmetros de autenticação do switch e do servidor de autenticação devem ser os mesmos.

Procedimento de configuração

Passo	Operação	Descrição
1	Conecte um servidor de autenticação no switch	Obrigatório, Registre as informações dos clientes para o servidor de autenticação e configure o nome de usuário e senha de autenticação correspondente para o cliente.
2	Instale um software 802.1X cliente	Obrigatório, Para os computadores, é necessário instalar o software cliente de autenticação 802.1X, disponível para download no site *http://www.intelbras.com.br*
3	Configuração global 802.1X	Obrigatório, Por padrão a função global 802.1X é desabilitado, Vá em Network Security⟶802.1X⟶Global Config, configure a função 802.1X globalmente.
4	Configure os parâmetros para a autenticação no servidor de autenticação	Obrigatório, em Network Security⟶802.1X⟶Radius Server, configure os parâmetros do servidor.
5	Configure o 802.1X para a porta.	Obrigatório, em Network Security⟶802.1X⟶Port Config, configure a função 802.1X para a porta do switch baseado em suas necessidades.

12. SNMP

» **Visão geral do SNMP**

SNMP (Simple Network Management Protocol) é amplamente utilizado por aplicações executadas em redes UDP/IP. O SNMP fornece uma estrutura de gerenciamento para monitorar e manter os dispositivos de rede. É utilizado para gerenciar automaticamente vários dispositivos distintos de rede. Atualmente, a maioria dos sistemas de gerenciamento de rede são baseados em SNMP. Com a função SNMP habilitado, os administradores de rede podem facilmente monitorar o desempenho da rede, detectar as falhas e configurar os dispositivos de rede.

» **Estrutura de gerenciamento SNMP**

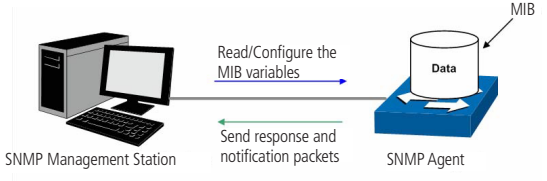
A estrutura de gerenciamento SNMP inclui três elementos de rede: estação de gerenciamento SNMP, agente SNMP e MIB (Management Information Base).

SNMP management station: Estação de Gerenciamento SNMP é a estação de trabalho que executa o programa cliente SNMP, fornecendo uma interface de gerenciamento amigável para o administrador gerenciar os dispositivos de rede mais conveniente.

SNMP agent: Agente SNMP é o processo executado pelo dispositivo de rede responsável por receber e processar os pacotes de solicitação da estação de gerenciamento SNMP. O Agente SNMP também poderá informar a estação de gerenciamento SNMP sobre possíveis eventos ocorridos com o dispositivo.

MIB: a MIB (Management Information Base) é a base de informações de gerenciamento. O agente é capaz de responder ao gerente consultas SNMP sobre o conjunto de informações contido na MIB. Cada agente SNMP possui sua própria MIB. A estação de gerenciamento SNMP pode ler ou escrever os objetos da MIB com base em seus direitos de gestão.

Estação de gerenciamento SNMP é o gerente da rede SNMP, enquanto o agente SNMP é o objeto gerenciado. As informações entre a estação de gerenciamento SNMP e o agente SNMP são trocadas através do protocolo SNMP (Simple Network Management Protocol). A relação entre a estação de gerenciamento SNMP, agente SNMP e a MIB, é ilustrado na figura a seguir.



Relação entre os elementos de rede SNMP

» **Versões SNMP**

Este switch suporta SNMP v3 que é compatível com SNMP v1 e SNMP v2c. As versões do SNMP adotadas pela Estação de Gerenciamento e o Agente SNMP devem ser a mesma. Caso contrário, a Estação de Gerenciamento SNMP e o Agente SNMP podem não se comunicar corretamente. Você pode selecionar o modo de gerenciamento com níveis de segurança adequado as suas exigências de aplicação.

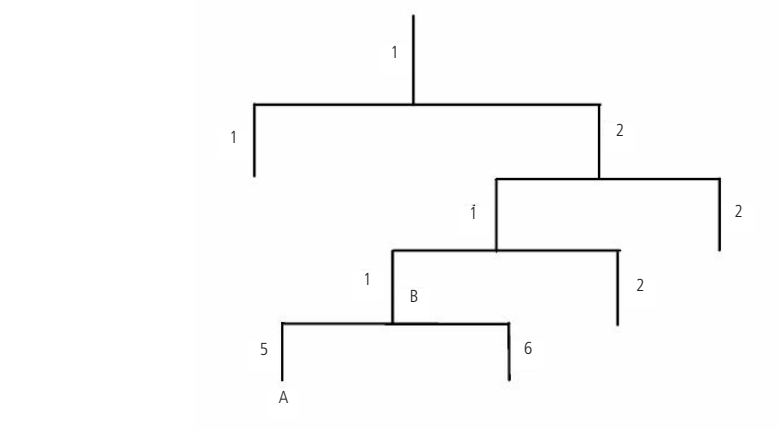
SNMP v1: o SNMPv1 adota autenticação utilizando o nome da comunidade. O nome da comunidade é usado para definir a relação entre a estação de gerenciamento SNMP e o agente SNMP. Os pacotes SNMP que não conseguirem aprovação de autenticação serão descartados.

SNMP v2c: também adota a autenticação utilizando o nome da comunidade. É compatível com SNMP v1, com algumas funcionalidades a mais, como implementação de comunicação Gerente-Gerente e aumento no nível de segurança.

SNMP v3: baseado em SNMP v1 e v2c, o SNMPv3 aumenta em muito a segurança e capacidade de gerenciamento. Adota autenticação VACM (View-based Access Control Model) e USM (User-Based Security Model). O usuário pode configurar a autenticação e as funções de criptografia. A função de autenticação é utilizada para limitar o acesso de usuários ilegais, autenticando o remetente do pacote. Enquanto isso, a função de criptografia é usada para criptografar os pacotes transmitidos entre a estação de gerenciamento SNMP e o agente SNMP, de modo a evitar que qualquer informação seja capturada. As múltiplas combinações da função de autenticação e criptografia garantem uma comunicação mais confiável entre a estação de gerenciamento SNMP e o agente SNMP.

» **Introdução MIB**

Para identificar os objetos de gerenciamento dos dispositivos em mensagens SNMP, o SNMP adota uma arquitetura hierárquica. É como se fosse uma árvore, e que cada nó da árvore representasse um objeto. Assim, o objeto pode ser identificado como único caminho a partir da raiz, e é indicado por uma sequencia de números. A sequência de números é o identificador do objeto. Na figura a seguir o OID do objeto gerenciado B é {1.2.1.1}. Enquanto o OID do objeto gerenciado A é {1.2.1.1.5}.



Arquitetura das MIBs

» **Configuração do SNMP**

1. **Create view**

   A view do SNMP é criada para a estação de gerenciamento SNMP gerenciar objetos da MIB. Os objetos gerenciados são identificados exclusivamente pelo seu OID. O OID do objeto gerenciado pode ser encontrado no programa cliente SNMP em execução na estação de gerenciamento SNMP.

2. **Create SNMP group**

   Após criada a view SNMP, é necessário que se crie um grupo SNMP. O nome do grupo, versão do protocolo SNMP e o nível de segurança compõem o identificador do grupo SNMP. Você pode configurar grupos SNMP para controlar o acesso à rede, fornecendo aos usuários em vários grupos distintos, várias formas de gerência, como por exemplo, leitura, escrita e notificação.

3. **Criação de usuários SNMP**

   O usuário que está em um grupo SNMP, pode gerenciar o switch através do programa cliente na estação de gerenciamento. O nome de usuário e a senha são utilizados para as estações de gerenciamentos SNMP, isso para terem acesso aos agentes SNMP.

O menu SNMP é utilizado para configurar a função de SNMP do switch, incluindo 3 sub-menus de configuração: *SNMP Config, Notification* e *RMON*.

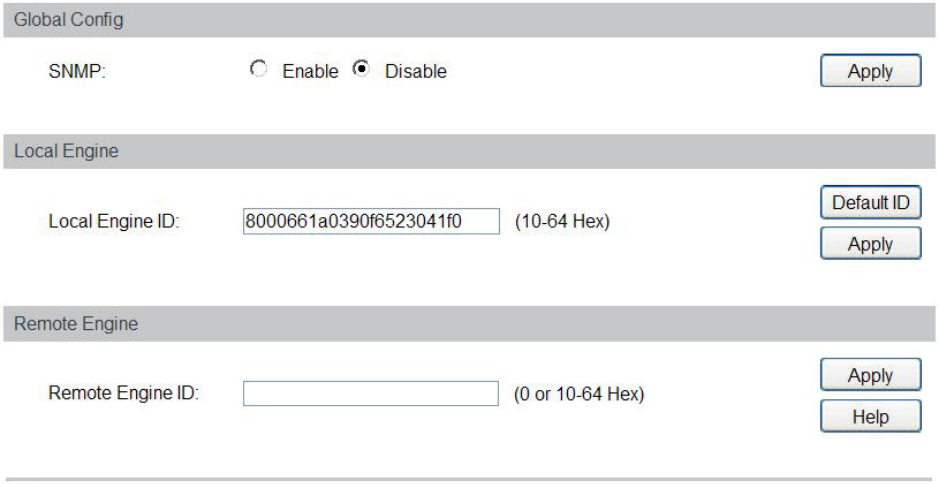
12.1. SNMP config

As configurações SNMP podem ser configuradas nas seguintes páginas de configuração: Global Config, SNMP View, SNMP Group, SNMP User e SNMP Community.

Global config

Esta página é utilizada para habilitar globalmente a função SNMP do switch.

Escolha o menu *SNMP → SNMP Config → Global Config* para carregar a página seguinte:



Global config

As seguintes opções são apresentadas na tela.

» **Global config**

SNMP: selecione *Enable/Disable* para habilitar ou desabilitar a função SNMP.

» **Local Engine**

Local Engine ID: digite a identificação do SNMP Engine do switch Local, este parâmetro é utilizado pelos clientes remotos. O engine ID é uma sequência de carácteres alfanuméricos únicos, usado para identificar o switch.

» **Remote Engine**

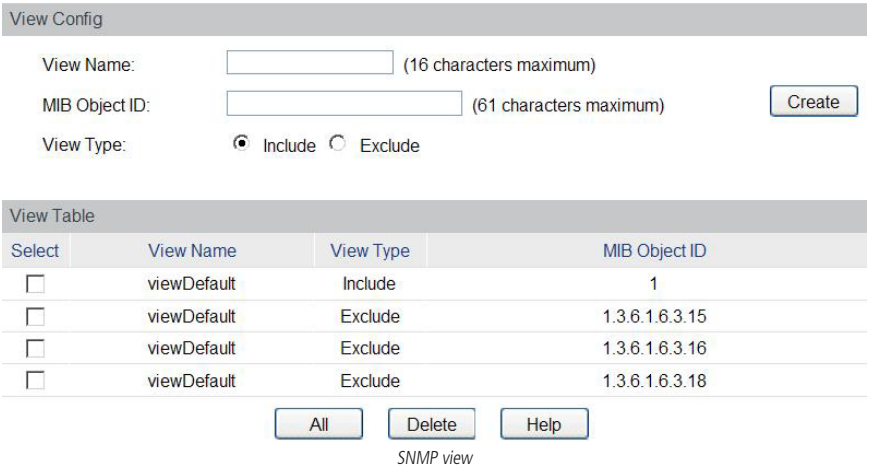
Remote Engine ID: digite a identificação do SNMP Engine do switch remoto (o Remote Engine é utilizado para o envio de snmp inform V3 para o switch ou dispositivo remoto SNMP v3). O engine ID é uma sequência de caracteres alfanuméricos únicos, usado para identificar o switch.

Obs.: *a quantidade de caracteres para identificação do Engine ID deve ser o mesmo.*

SNMP view

O OID (Object Identifier) dos pacotes SNMP são usado para descrever os objetos gerenciados do switch, e as MIB (Management Information Base) é o conjunto dos OIDs. O SNMP view é criado para a estação de gerenciamento SNMP gerenciar os objetos MIB.

Escolha o menu *SNMP → SNMP Config → SNMP View* para carregar a seguinte página.



SNMP view

As seguintes informações são apresentadas na tela:

» **View config**

View name: digite o nome de identificação da view. Cada view pode incluir várias entradas com o mesmo nome.

MIB object ID: digite o OID utilizado pela view.

View type: selecione o tipo de entrada da view.

» Include: inclui para o gerenciamento o OID especificado para a view.

» Exclude: exclui o gerenciamento o OID especificado para a view.

» **View table**

Select: selecione a entrada desejada e clique no botão *Delete* para remover a view desejada. Todas as entradas de uma mesma view, serão excluídas juntas.

View name: exibe o nome da view.

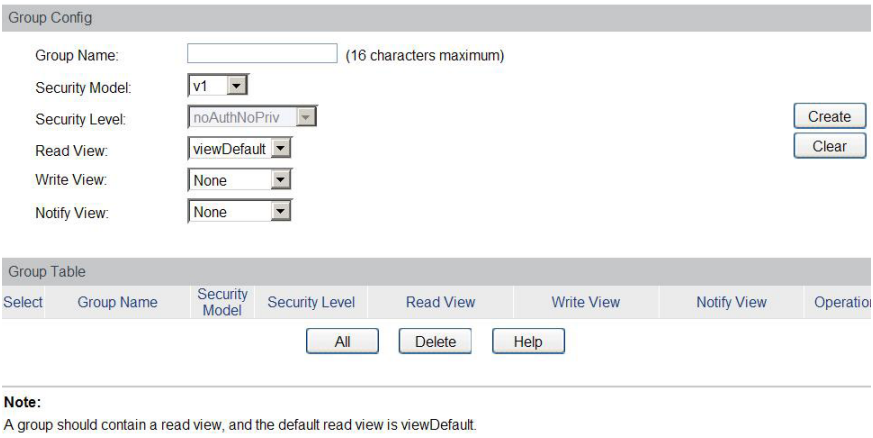
View type: exibe o tipo de entrada da view.

MIB object ID: exibe o OID da view.

SNMP group

Nesta página você pode configurar grupos SNMP para controlar o acesso à rede, fornecendo aos usuários de vários grupos diferentes, permissões de leitura, escrita e notificação.

Escolha no menu *SNMP* → *SNMP Config* → *SNMP Group* para carregar a seguinte página.



As seguintes informações são apresentadas na tela.

» **Group config**

Group name: digite o nome do grupo SNMP.

Security model: selecione a versão do protocolo SNMP utilizado pelo grupo SNMP.

» V1: nesta versão, o nome da comunidade é utilizado para a autenticação. O SNMP v1 pode ser configurado diretamente na página de configuração SNMP Community.

» V2C: nesta versão, o nome da comunidade é utilizado para a autenticação. O SNMP v2c pode ser configurado diretamente na página de configuração SNMP Community.

» V3: nesta versão, o mecanismo USM é utilizado para realizar a autenticação. Ao habilitar o SNMP v3, o campo nível de segurança deverá ser configurado.

Security level: selecione o nível de segurança para grupos SNMPv3.

» noAuthNoPriv: este nível de segurança não realiza autenticação e criptografia.

» authNoPriv: este nível de segurança realiza autenticação porém não realiza criptografia.

» AuthPriv: este nível de segurança realiza autenticação e criptografia.

Read view: selecione a view desejada com acesso somente de leitura. A view definida como read somente poderá ser lida, não é possível modificá-la.

Write view: selecione a view desejada com acesso de escrita. A view definida como write poderá ser lida e alterada.

Notify view: selecione a view desejada com permissão de notificação. A view definida como notify poderá enviar notificações a estação de gerenciamento SNMP.

» **Group table**

Select: selecione a entrada desejada e clique no botão *Delete* para remover o grupo SNMP desejado.

Group name: exibe o nome do grupo SNMP.

Security model: exibe a versão do protolo SNMP utilizada pelo grupo SNMP.

Security level: exibe o nível de segurança do grupo SNMP.

Read view: exibe a view de leitura.

Write view: exibe a view de escrita

Notify view: exibe a view de notificação.

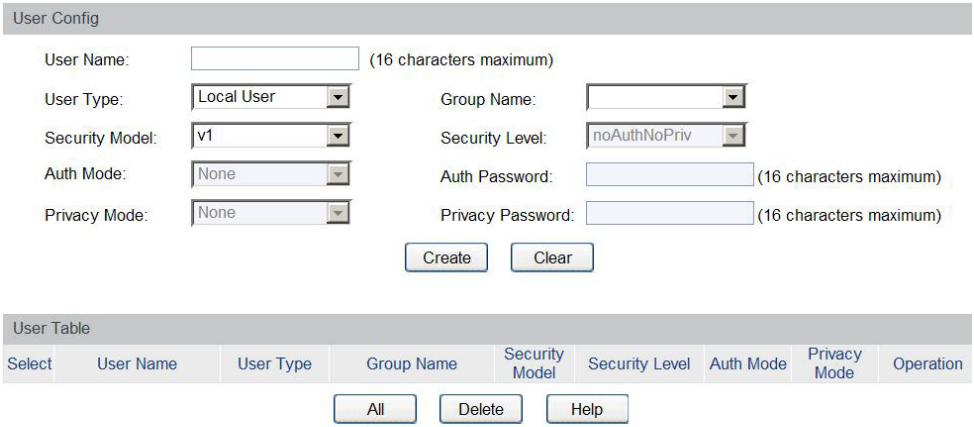
Operation: clique no botão *Edit* para modificar a view desejada. Após realizado a modificação clique em *Modify* para validar a alteração.

Obs.: *cada grupo deve conter uma view de leitura. A view de leitura padrão é view Default.*

SNMP User

Nesta página é possível configurar o nome de usuário que gerenciará o grupo SNMP. O usuário e grupo SNMP devem possuir o mesmo nível de segurança e direito de acesso.

Escolha o menu *SNMP → SNMP Config → SNMP User* para carregar a seguinte página:



Note:
The security model and security level of the user should be the same with that of its group.

Usuários SNMP

As seguintes informações são exibidas na tela:

» **User config**

User name: digite o nome de usuário.

User type: selecione o tipo de usuário.

» Local User: indica que o usuário está conectado ao SNMP Engine local.

» Remote User: indica que o usuário está conectado ao SNMP Engine remoto.

Group name: selecione o grupo SNMP desejado. O usuário é classificado para o grupo correspondente de acordo com o *Group Name, Security Model e Security Level*.

Security model: selecione a versão do protocolo SNMP utilizada pelo usuário criado.

Security level: selecione o nível de segurança para o usuário SNMP v3.

Auth mode: selecione o modo de autenticação para o usuário SNMP v3.

» None: nenhum método de autenticação é usado.

» MD5: a autenticação da porta usa o algoritmo HMAC-MD5.

» SHA: a autenticação da porta é realizada através de SHA (Secure Hash Algorithm). Esse modo de autenticação tem uma segurança maior que o modo MD5.

Auth password: digite a senha configurada para autenticação.

Privacy mode: selecione o modo de criptografia para o usuário SNMP v3.

» None: nenhum método de privacidade é utilizado.

» DES: utiliza o método de encriptação DES.

Privacy password: digite a senha configurada utilizada na criptografia.

» **User Table**

Select: selecione a entrada desejada e clique no botão *Delete* para remover o usuário SNMP desejado.

User name: exibe o nome do usuário.

User type: exibe o tipo de usuário.

Group name: exibe o nome do grupo do usuário.

Security model: exibe o modo de segurança do usuário.

Security level: exibe a versão do protocolo SNMP utilizado pelo usuário.

Auth mode: exibe o modo de autenticação do usuário.

Privacy mode: exibe o modo de privacidade do usuário.

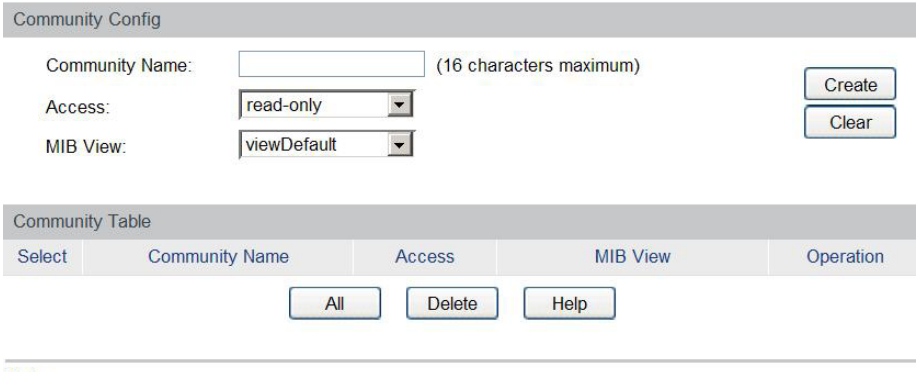
Operation: clique no botão *Edit* para modificar o grupo do usuário e clique no botão *Modify* para aplicar as configurações.

Obs.: *o usuário e grupo SNMP devem possuir o mesmo modo e nível de segurança.*

SNMP community

O SNMP v1 e v2c utiliza o método de autenticação baseado no nome da comunidade. O nome da comunidade pode limitar o acesso ao agente SNMP da estação de gerenciamento SNMP, funcionando como uma senha. Caso a versão do protocolo utilizada for, SNMP v1 ou SNMP v2c, é possível configurar a função utilizando somente esta página sem a necessidade de configurar as páginas SNMP Group e USER SNMP.

Escolha o menu *SNMP* → *SNMP Config* → *SNMP Community* para carregar a seguinte página:



Comunidades SNMP

As seguintes opções são apresentadas na tela:

» **Community config**

Community name: digite o nome da comunidade.

Access: defina o tipo de permissão para a comunidade.

» Read-only: neste modo, a comunidade terá permissão somente de leitura, nenhuma alteração poderá ser feita.

» Read-write: neste modo, a comunidade terá permissão de leitura e escrita, podendo realizar alterações.

MIB View: selecione a view de acesso da comunidade.

» **Community table**

Select: selecione a entrada desejada e clique no botão *Delete* para remover a comunidade desejada.

Community name: exibe o nome da comunidade.

Access: exibe o tipo de permissão da comunidade para acessar a view.

MIB view: exibe a view que a comunidade pode acessar.

Operation: clique no botão *Edit* para modificar a view e a permissão de acesso da comunidade, em seguida, clique no botão *Modify* para aplicar as configurações.

Obs.: *a view padrão para a comunidade SNMP é viewDefault.*

Procedimento de configuração:

» Caso for utilizado o SNMPv3, por favor, siga os seguintes passos.

Passo	Operação	Descrição
1	Habilita a função global SNMP	Obrigatório, em SNMP → SNMP Config → Global Config, habilite a função SNMP.
2	Crie SNMP view	Obrigatório, em SNMP → SNMP Config → SNMP View, crie uma view SNMP para o agente de gerenciamento. O nome da view padrão é viewDefault e o OID padrão é 1.
3	Crie o grupo SNMP	Obrigatório, em SNMP → SNMP Config → SNMP Group, crie um grupo SNMP e especifique as views e o nível de segurança desejado.
4	Crie o usuário SNMP	Obrigatório, em SNMP → SNMP Config → SNMP user, crie o usuário SNMP para o grupo e configure o nível de segurança para o usuário.

» Caso for utilizado o SNMP v1 ou SNMP v2c, por favor, siga os seguintes passos.

Passo	Operação		Descrição
1	Habilita a função global SNMP		Obrigatório, em SNMP ⟶ SNMP Config ⟶ Global Config, habilite a função SNMP.
2	Crie SNMP view		Obrigatório, em SNMP ⟶ SNMP Config ⟶SNMP View, crie uma view SNMP para o agente de gerenciamento. O nome da view padrão é viewDefault e o OID padrão é 1.
3	Configure o nível de acesso para o usuário	Criar a comunidade SNMP diretamente.	- Criar a comunidade diretamente. Em SNMP⟶SNMP Config⟶SNMP Community, criar a comunidade baseada em SNMP v1 e SNMPv2c
		Criar o grupo e usuário SNMP.	- Criar grupo e usuário SNMP. Semelhante à configuração do SNMPv3, você pode criar grupos e usuários SNMPv1/v2c. O nome de usuário limita o acesso aos agentes SNMP e a estação de gerenciamento SNMP. Funciona como o nome de comunidade. Os usuários podem gerenciar os dispositivos através de views de leituras, escritas e notificações definidas nos grupos SNMP.

12.2. Notification

Com a função de notificação habilitada, o switch podem intuitivamente reportar as estações de gerenciamento SNMP, eventos que ocorreram nas views (ex. Dispositivos reiniciados) permitindo que as estações de gerenciamento monitorem e processem os eventos.

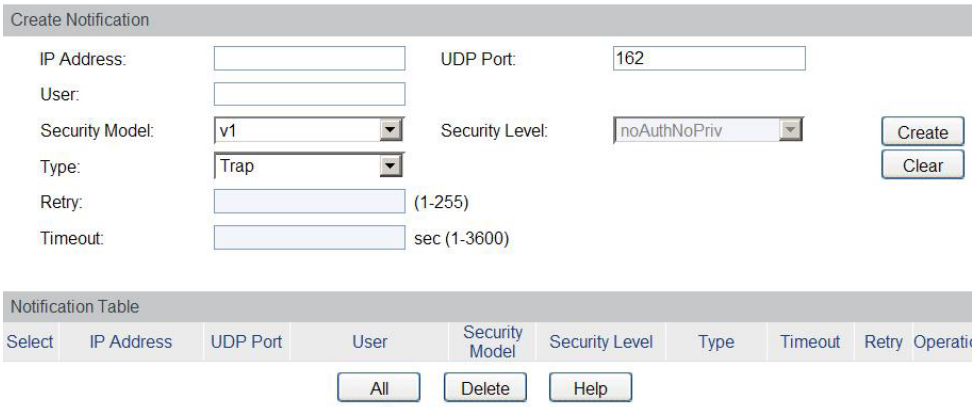
As informações de notificação incluem os seguintes tipos:

Trap: é a informação que o dispositivo gerenciado envia para a estação de gerenciamento de rede sem nenhum tipo de solicitação.

Inform: pacotes inform são enviados para informar a estação de gerenciamento sobre eventuais eventos, e aguardar uma resposta. A notificação Inform somente é utilizada com o SNMP v3 e possui uma maior segurança comparado ao Trap.

Nesta página, você pode configurar as notificações da função SNMP.

Escolha o menu *SNMP* ⟶ *Notification* ⟶ *Notification* para carregar a seguinte página:



Notification

As seguintes opções são apresentadas na tela:

» **Create notification**

IP address: digite o endereço da estação de gerenciamento SNMP.

UDP port: digite o número da porta UDP usada para enviar notificações. Padrão é *162*.

User: digite o nome de usuário da estação de gerenciamento.

Security model: selecione a versão do protocolo SNMP.

Security level: selecione o nível de segurança para grupos SNMPv3.

» noAuthNoPriv: este nível de segurança não realiza autenticação e criptografia.

» authNoPriv: este nível de segurança realiza autenticação porém não realiza criptografia.

» AuthPriv: este nível de segurança realiza autenticação e criptografia.

Type: selecione o tipo de notificação.

» Trap: indica que o tipo de notificação utilizada é a Trap.

» Inform: indica que o tipo de notificação utilizada é a Inform. O tipo Inform tem uma maior segurança em relação ao tipo Trap.

Retry: indica a quantidade de vezes que o switch reenvia uma solicitação inform.

Timeout: específica um tempo máximo para o switch esperar pela resposta da estação de gerenciamento SNMP antes de reenviar um pedido.

» **Notification table**

Select: selecione a estação de gerenciamento desejado e clique no botão *Delete* para remover a entrada desejada.

IP address: exibe o endereço IP da estação de gerenciamento SNMP.

UDP port: exibe a porta UDP usada para notificações.

User: exibe o nome de usuário da estação de gerenciamento.

Security model: exibe a versão do protocolo SNMP.

Security level: exibe o nível de segurança do SNMPv3.

Type: exibe o tipo de notificações.

Timeout: exibe o tempo máximo para o switch esperar pela resposta da estação de gerenciamento SNMP antes de reenviar um pedido.

Retry: exibe a quantidade de vezes que o switch reenvia uma solicitação inform.

Operation: clique no botão *Edit* para realizar modificações e no botão *Modify* para aplicar as alterações.

12.3. RMON

RMON (Remote Monitoring) é baseado na arquitetura SNMP (Simple Network Management Protocol). RMON é atualmente um padrão de gerenciamento de rede definido pelo Internet Engineering Task Force (IETF), é utilizado principalmente para monitorar o tráfego de dados através de uma segmento de rede ou até mesmo de toda a rede, de modo a permitir que o administrador da rede possa tomar as medidas de proteção a tempo de evitar qualquer mau funcionamento da rede. Além disso, as MIB RMON registram informações estatísticas de desempenho da rede e mau funcionamento periodicamente, com base no que as estações de gerenciamento podem monitorar. RMON é útil para administradores de rede, para gerenciar a rede em grande escala, uma vez que reduz o tráfego de comunicação entre as estações de gerenciamento e os agentes de gerenciamento.

» Grupos RMON

Este switch suporta os seguintes grupos RMON definidos no padrão (RFC1757), History Group, Event Group, Statistic Group e Alarm Group.

Grupo RMON	Função
Grupo History	Após configurado o grupo History, o switch coleta e registra periodicamente informações de estatísticas de rede, baseado no que as estações de gerenciamento podem informar de forma eficaz.
Grupo Event	O grupo Event é utilizado para definir eventos RMON. Alarmes ocorrem quando um evento é detectado.
Grupo Statistic	O grupo Statistic é utilizado para monitorar as estatísticas das variáveis de alarme nas portas especificadas.
Grupo Alarm	O grupo Alarm é utilizado para monitorar variáveis específicas de alarme. Quando o valor de uma variável exceder o limite previamente estabelecido, um evento de alarme será gerado.

Os grupos RMON podem ser configurados em History Control, Event Config e Alarm Config.

History control

Nesta página você pode configurar o grupo History da função RMON.

Escolha o menu *SNMP → RMON → History Control* para carregar a página seguinte:

History Control Table

Select	Index	Port	Interval (sec)	Owner	Status
☐		Port 1			Disable
☐	1	Port 1	1800	monitor	Disable
☐	2	Port 1	1800	monitor	Disable
☐	3	Port 1	1800	monitor	Disable
☐	4	Port 1	1800	monitor	Disable
☐	5	Port 1	1800	monitor	Disable
☐	6	Port 1	1800	monitor	Disable
☐	7	Port 1	1800	monitor	Disable
☐	8	Port 1	1800	monitor	Disable
☐	9	Port 1	1800	monitor	Disable
☐	10	Port 1	1800	monitor	Disable
☐	11	Port 1	1800	monitor	Disable
☐	12	Port 1	1800	monitor	Disable

Apply Help

Grupo History

» **History control table**

Select: selecione a entrada desejada para configuração.
Index: exibe o índice da entrada.
Port: selecione a porta desejada.
Interval: especifique o intervalo de coleta das amostras.
Owner: digite o nome do dispositivo ou usuário que definiu a regra.
Status: selecione *Enable/Disable* para habilitar ou desabilitar a entrada correspondente.

Event config

Nesta página você pode configurar o grupo Event da função RMON.

Escolha o menu *SNMP → RMON → Event Config* para carregar a página seguinte:

Event Table

Select	Index	User	Description	Type	Owner	Status
☐				None		Disable
☐	1	public		None	monitor	Disable
☐	2	public		None	monitor	Disable
☐	3	public		None	monitor	Disable
☐	4	public		None	monitor	Disable
☐	5	public		None	monitor	Disable
☐	6	public		None	monitor	Disable
☐	7	public		None	monitor	Disable
☐	8	public		None	monitor	Disable
☐	9	public		None	monitor	Disable
☐	10	public		None	monitor	Disable
☐	11	public		None	monitor	Disable
☐	12	public		None	monitor	Disable

Apply Help

Grupo Event

As seguintes opções são apresentadas na tela:

» **Event table**

Select: selecione a entrada desejada para configuração.

Index: exibe o índice.

User: digite o nome do usuário ou a comunidade a qual pertence o evento.

Description: digite uma descrição para identificação.

Type: selecione o tipo de evento.

» None: nenhum processamento.

» Log: evento de Login.

» Notify: envio de mensagens Trap para a estação de gerenciamento.

» Log&Notify: registra eventos e envia mensagens Trap para a estação de gerenciamento.

Owner: digite o nome do dispositivo ou usuário que definiu regra.

Status: selecione *Enable/Disable* para habilitar ou desabilitar o evento correspondente.

Alarm config

Nesta página você pode configurar os grupos Statistics e Alarm da função RMON.

Escolha o menu *SNMP → RMON → Alarm Config* para carregar a seguinte página:

Alarm Table

Select	Index	Variable	Port	Sample Type	Rising Threshold	Rising Event	Falling Threshold	Falling Event	Alarm Type	Interval (sec)	Owner	Status
☐		DropEvents		Absolute					All			Disable
☐	1	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	2	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	3	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	4	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	5	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	6	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	7	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	8	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	9	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	10	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	11	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable
☐	12	DropEvents	Port 1	Absolute	100	0	100	0	All	1800	monitor	Disable

Apply Help

Grupo Alarm

As seguintes opções são apresentadas na tela:

» **Alarm table**

Select: selecione a entrada desejada para configuração.

Index: exibe o índice da entrada.

Variable: selecione as variáveis na lista.

Port: selecione a porta a qual a regra de alarme está associada.

Sample type: especifique o método de amostragem para a variável selecionada para comparar os valores entre os limites.

» Absolute: compara os valores diretamente com os limites no final do intervalo de amostragem.

» Delta: subtrai o último valor amostrado a partir do valor atual. A diferença nos valores é comparada como limite

Rising threshold: digite o valor para o contador disparar o alarme caso este valor seja excedido.

Rising event: selecione o índice do evento correspondente, que será acionado se o valor amostrado for maior que o Rising Threshold.

Falling threshold: digite o valor para o contador disparar o alarme caso esse valor seja menor que o especificado.

Falling event: selecione o índice do evento correspondente, que será acionado se o valor amostrado for menor que o Falling Threshold.

Alarm type: especifique o tipo de alarme.

» All: o evento será acionado se o valor amostrado ultrapassar o Rising Threshold ou estiver abaixo do Falling Threshold.

» Rising: quando o valor amostrado exceder o limite de Rising Threshold, um evento de alarme será acionado.

» Falling: quando o valor amostrado estiver abaixo do valor especificado no Falling Threshold, um evento de alarme será acionado.

Interval: digite o intervalo de tempo de alarme em segundos.

Owner: digite o nome do dispositivo ou usuário que definiu a entrada.

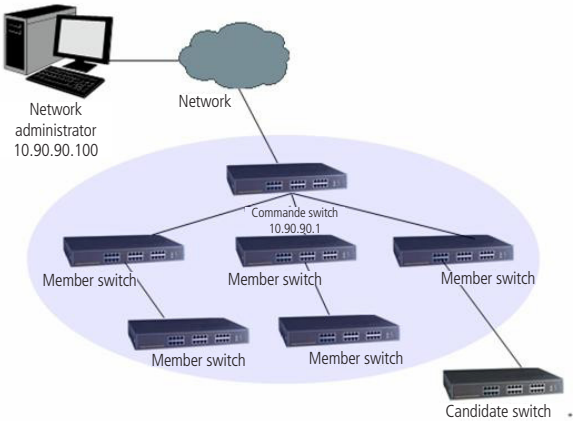
Status: selecione *Enable/Disable* para habilitar ou desabilitar a regra correspondente.

Obs.: *quando as variáveis excedem o limite de alarme continuamente, um evento de alarme será gerado somente na primeira vez.*

13. Cluster

Com o desenvolvimento das tecnologias, as redes foram ganhando grandes proporções, tornando-se necessário o aumento da quantidade de dispositivos e dificultando ainda mais a gestão destas redes. A função *Gerenciamento de Cluster* pode resolver esta questão. O administrador pode gerenciar e manter os switches no Cluster através do Commander Switch (Switch Principal). Este switch gerencia os demais switches da rede.

A figura a seguir, exibe uma topologia de cluster.



Topologia Cluster

» Cluster Role

De acordo com as suas funções e status, o cluster de switches desempenham papéis diferentes. Você pode estabelecer a função que o switch deverá exercer.

Commander switch: indica que o switch pode configurar e gerenciar todos os dispositivos através do cluster. Descobre e determina quais os switches estão presentes na rede através das informações coletadas pelos protocolos NDP (Neighbor Discovery Protocol) e NTDP (Neighbor Topology Discovery Protocol).

Member switch: indica os dispositivos gerenciados pelo Cluster.

Candidate switch: indica quais dispositivos não pertencem ao Cluster. Estes dispositivos podem ser incluídos no grupo.

Individual switch: indica o dispositivo com a função de cluster desativada.

As funções podem ser trocadas de um switch para o outro, seguindo as regras estabelecidas.

» O switch que você criar o cluster será o Commander Switch (Switch Principal).
» O Commander Switch (Switch Principal) descobre e determina quais os switches estão presentes na rede através de determinados protocolos.
» Após ser adicionado ao cluster, o switch candidate torna-se um switch member.
» Após ser removido do cluster, o switch member torna-se um switch candidate.
» O Commander Switch passa a ser o único switch candidate quando o cluster for excluído.

Introdução ao Cluster: a função de cluster utiliza três protocolos de gerenciamento: NDP (Neighbor Discovery Protocol), NTDP (Neighbor Topology Discovery Protocol) e CMP (Cluster Management Protocol).

» NDP: os switches utilizam o NDP para coletar informações dos switches diretamente conectados a ele, informações como, versão de Software, hostname, endereço MAC e número da porta conectada.
» NTDP: os switches utilizam o NTDP para coletar informações dos switches que não estão diretamente conectados a ele, informações referente a topologia da rede e dispositivos com NTDP ativo.
» CMP: protocolo utilizado pelo commander switch (Switch Principal) para gerenciamento dos switches dentro do cluster.

Obs.: *o switch SG 2404 MR não pode ser configurado como commander switch (Switch Principal) para gerenciar demais switches em cluster.*

13.1. NDP

Os switches utilizam o NDP para coletar informações dos switches diretamente conectados a ele, informações como, versão de software, hostname, endereço MAC e número da porta conectada. O switch principal mantém uma tabela com estas informações. Caso sejam adicionados mais dispositivos na rede, o NDP coleta os dados e inclui na tabela. Caso seja retirado algum dispositivo, o NDP atualizará a tabela, removendo os dados do dispositivo antigo.

Esta função pode ser implementada nas páginas *Neighbor Info, NDP Summary* e *NDP Config.*

Neighbor info

Nesta página você pode visualizar as informações coletadas pelo NDP de um switch:

Escolha o menu *Cluster* → *NDP* → *Neighbor Info* para carregar a seguinte página:

Informações dos vizinhos

As seguintes opções são exibidas na tela:

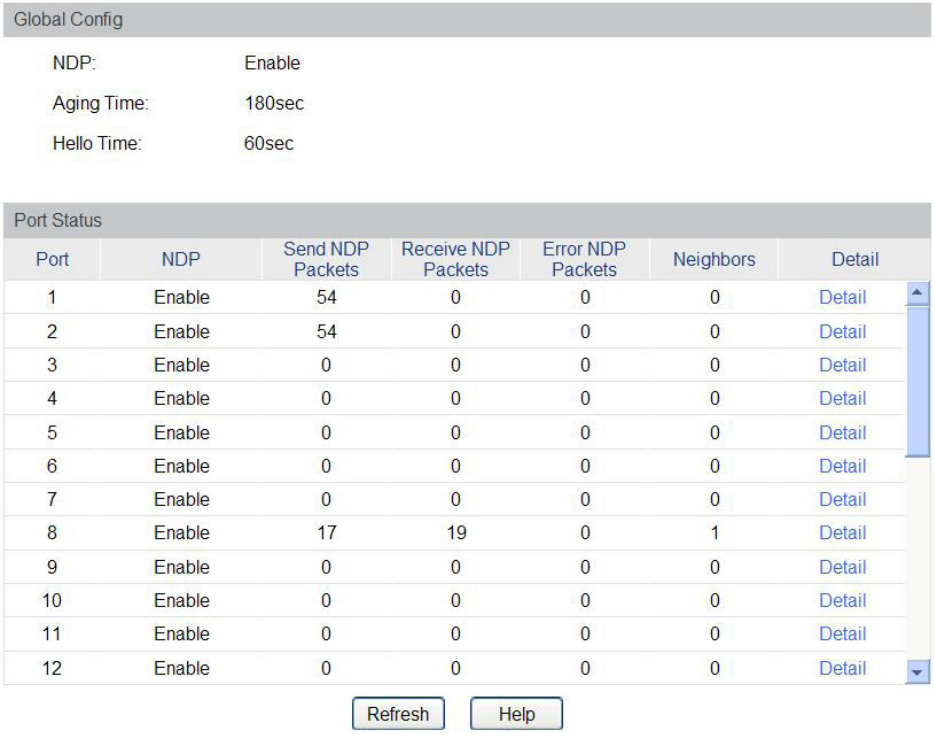
» **Neighbor Search**
Search Option: selecione a informação desejada. Em seguida, clique no botão *Search* para exibir as informações da tabela.

» **Neighbor Info**
Native Port: exibe o número da porta do switch.
Remote Port: exibe o número da porta que o switch está conectado na rede.
Device Name: exibe o nome do switch conectado na rede.
Device MAC: exibe o endereço MAC do switch conectado na rede.
Firmware Version: exibe a versão do firmware do switch conectado na rede.
Aging Time: exibe o período que o switch principal manterá a as informações do switch conectado à rede.

NDP summary

Nesta página você visualizar a configuração do NDP do switch.

Escolha o menu *Cluster* → *NDP* → *NDP Summary* para carregar a seguinte página:


Global Config
NDP: Enable
Aging Time: 180sec
Hello Time: 60sec
Port Status
Port NDP Send NDP Packets Receive NDP Packets Error NDP Packets Neighbors Detail
1 Enable 54 0 0 0 Detail
2 Enable 54 0 0 0 Detail
3 Enable 0 0 0 0 Detail
4 Enable 0 0 0 0 Detail
5 Enable 0 0 0 0 Detail
6 Enable 0 0 0 0 Detail
7 Enable 0 0 0 0 Detail
8 Enable 17 19 0 1 Detail
9 Enable 0 0 0 0 Detail
10 Enable 0 0 0 0 Detail
11 Enable 0 0 0 0 Detail
12 Enable 0 0 0 0 Detail
Refresh
Help

Estatísticas NDP

As seguintes opções são exibidas na tela:

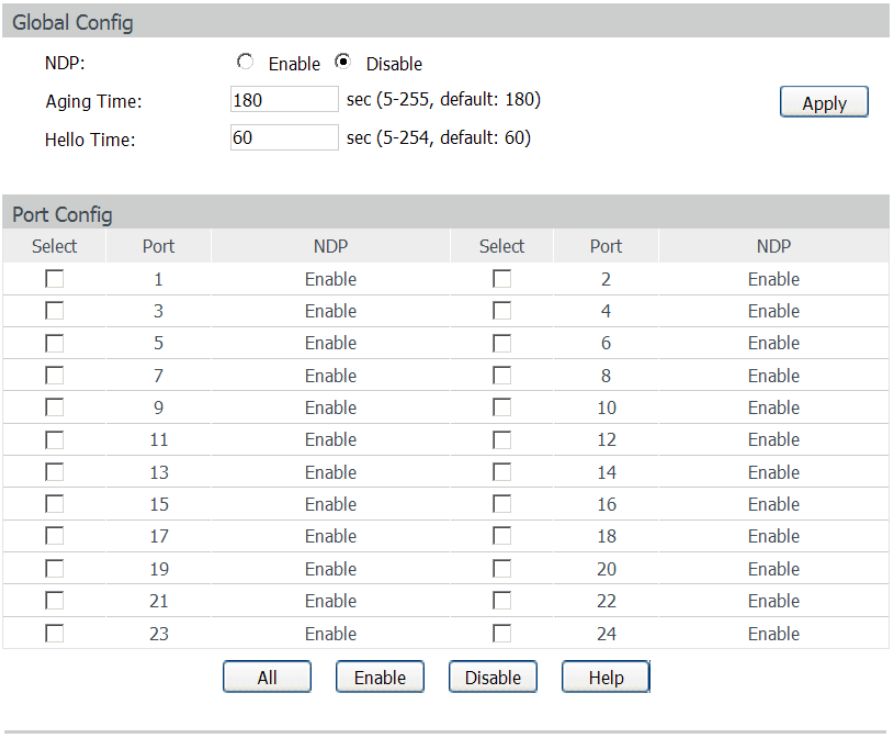
» **Global config**
NDP: exibe o status do NDP (Ativado/Desativado).
Aging time: exibe o período que será mantido os pacotes de informações de um switch conectado a rede.
Hello time: exibe o período de coleta das informações dos dispositivos conectados à da rede.

» **Port status**
Port: exibe o número da porta do switch.
NDP: exibe o status do NDP (Ativado/Desativado) na porta desejada.

Send NDP packets: exibe a contagem de pacotes NDP enviados.
Receive NDP packets: exibe a contagem de pacotes NDP recebidos.
Error NDP packets: exibe a contagem de pacotes de erro NDP recebidos.
Neighbors: exibe a contagem de dispositivos conectados a rede.
Detail: exibe as informações completa coletada pela porta.

NDP config

Nesta página você pode configurar a função NDP.
Escolha o menu *Cluster* → *NDP* → *NDP Config* para carregar a seguinte página:


Global Config
NDP: Enable Disable
Aging Time: 180 sec (5-255, default: 180)
Hello Time: 60 sec (5-254, default: 60)
Apply
Port Config
Select Port NDP Select Port NDP
1 Enable 2 Enable
3 Enable 4 Enable
5 Enable 6 Enable
7 Enable 8 Enable
9 Enable 10 Enable
11 Enable 12 Enable
13 Enable 14 Enable
15 Enable 16 Enable
17 Enable 18 Enable
19 Enable 20 Enable
21 Enable 22 Enable
23 Enable 24 Enable
All Enable Disable Help

Configuração NDP

As seguintes opções são exibidas na tela:

» **Global config**
NDP: selecione o status do NDP (Ativado/Desativado).
Aging time: digite o período que será mantido os pacotes de informações de um switch conectado a rede.
Hello time: digite o intervalo para coleta de informações da rede através do NDP.

» **Port config**
Select: selecione a porta que deseja habilitar o NDP.
Port: exibe o número da porta do switch.
NDP: exibe o status do NDP (Ativado/Desativado) na porta desejada.
Enable: habilita o NDP para a porta selecionada.
Disable: desabilita o NDP para a porta selecionada.

Obs.: *» A função NDP é eficaz somente quando a função está habilitada para a porta selecionada.*
» O Aging Time deve ser preenchido para que a informação da tabela do dispositivo conectado à rede não fique instável.

13.2. NTDP

Os switches utilizam o NTDP para coletar informações dos switches que não estão diretamente conectados a ele, informações referente a topologia da rede e dispositivos com NTDP ativo.

NTDP hop delay: indica o tempo de resposta entre a solicitação do switch principal e o recebimento dos pacotes informando os saltos dos dispositivos conectados à rede.

NTDP port delay: indica o tempo de resposta entre a porta que solicita os pacotes do switch principal e o recebimento dos pacotes enviados pelos switches conectados diretamente à rede.

A função NTDP pode ser implementada na página *Device Table, NTDP Summary* e *NTDP Comfit.*

Device table

Nesta página você pode visualizar as informações dos switches conectados diretamente às redes, coletadas através do NTDP. Não importa se o Cluster está estabelecido. Você pode receber as informações NTDP a qualquer momento para gerenciar estes dispositivos.

Selecione o menu *Cluster* → *NTDP* → *Device Table* para carregar a seguinte página:

Device Table

Device Type	Device MAC	Cluster Name	Role	Hops	Neighbor Info
1.0	90-F6-52-98-E9-AF		Candidate	1	Detail
1.0	90-F6-52-30-41-F0		Candidate	0	Detail

Collect Topology | Refresh | Help

Tabela de dispositivos

As seguintes opções são exibidas na tela:

» **Device table**

Device type: exibe a descrição coletada do dispositivo através do NTDP.

Device MAC: exibe o endereço MAC do dispositivo.

Cluster name: exibe o nome do Cluster do dispositivo.

Role: exibe a função que o dispositivo reproduz no cluster.

» **Commander Switch (switch principal):** indica o dispositivo que pode configurar e gerenciar todos os dispositivos no Cluster.

» **Member:** indica o dispositivo que é membro do Cluster.

» **Candidate:** indica os dispositivos que não estão incluídos no Cluster. Será possível adicionar.

» **Individual:** indica os dispositivos que estão com a função de Cluster desativada.

Hops: exibe a contagem de saltos do dispositivo até o Switch Principal.

Neighbor info: clique no botão *Detail* para visualizar todas as informações dos dispositivos.

Collect topology: clique em *Collect Topology* para o NTDP coletar as informações dos switches e de sua topologia de re mais recente.

Clique no botão *Detail* para visualizar todas as informações dos dispositivos.

Current Device Info

Device Name:	SF 2842 MR
MAC:	90-F6-52-30-41-F0
Hops:	1
Device Type:	1.0
IP Address:	192.168.0.2
Firmware Version:	1.0.0 Build 20120720 Rel.37087
Cluster Info:	Candidate

Neighbor Info

Native Port	Remote Port	Device MAC	Speed (Mbit/s)	Duplex
Port 08	Port 16	90-F6-52-98-E9-AF	100	FullDuplex

Back

Informações do dispositivo corrente

NTDP summary

Nesta página você pode visualizar a configuração do NTDP.

Escolha o menu *Cluster* → *NTDP* → *NTDP Summary* para carregar a seguinte página:

Global Config

NTDP:	Disable
NTDP Interval Time:	1min
NTDP Hops:	3hop
NTDP Hop Delay:	200ms
NTDP Port Delay:	20ms

Port Status

Port	NTDP	Port	NTDP
1	Enable	2	Enable
3	Enable	4	Enable
5	Enable	6	Enable
7	Enable	8	Enable
9	Enable	10	Enable
11	Enable	12	Enable
13	Enable	14	Enable
15	Enable	16	Enable
17	Enable	18	Enable
19	Enable	20	Enable
21	Enable	22	Enable
23	Enable	24	Enable

Refresh Help

Sumário NTDP

» **Global Config**

NTDP: exibe o status do NTDP Habilitado / Desabilitado.

NTDP interval time: exibe o intervalo de tempo para coletar as informações de topologia.

NTDP hops: exibe a contagem de saltos da topologia coletada.

NTDP hop delay: indica o tempo de resposta entre a solicitação do switch principal e o recebimento dos pacotes informando os saltos dos dispositivos conectados à rede.

NTDP port delay: indica o tempo de resposta entre a porta de solicitação de pacotes do switch principal e o recebimento dos pacotes enviados pelos switches conectados diretamente à rede.

» **Port status**

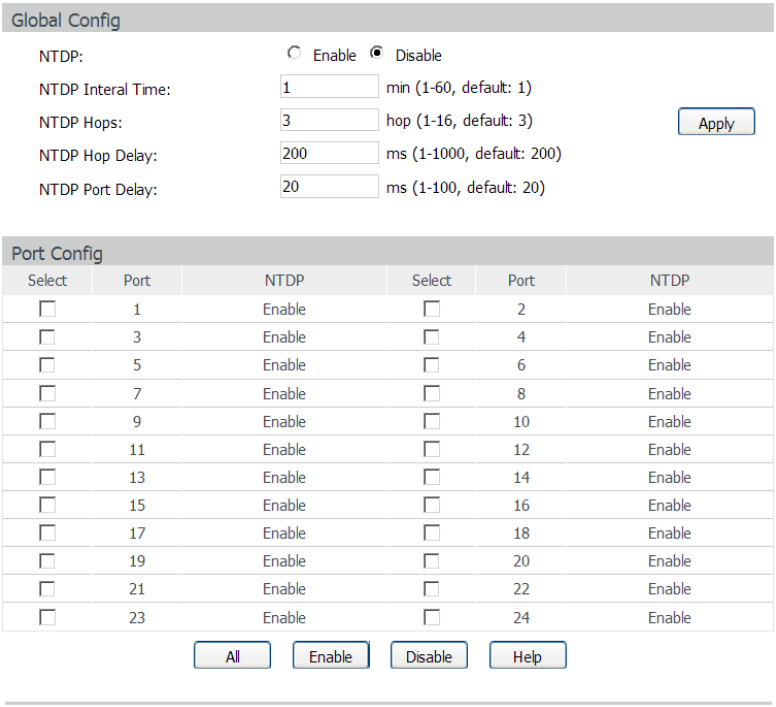
Port: exibe o número da porta do switch.

NTDP: exibe o status do NTDP Habilitado / Desabilitado desejada.

NTDP config

Nesta página você pode configurar o NTDP.

Escolha o menu *Cluster* → *NTDP* → *NTDP Config* para carregar a seguinte página:



Configuração NTDP

As seguintes opções são exibidas na tela:

» **Global config**

NTDP: selecione Habilitado / Desabilitado.

NTDP interval time: selecione o intervalo de tempo para coleta de informações da topologia da rede.

NTDP hops: digite a contagem de saltos coletados na topologia.

NTDP hop delay: digite o tempo de resposta entre a solicitação do switch principal e o recebimento dos pacotes informando os saltos dos dispositivos conectados à rede.

NTDP port delay: indique o tempo de resposta entre a porta de solicitação de pacotes do switch principal e o recebimento dos pacotes enviados pelos switches conectados diretamente à rede.

» **Port config**

Select: selecione a porta desejada para ativar o NDTP.

Port: exibe o número da porta do switch.

NTDP: exibe o status Habilitado / Desabilitado do NTDP.

Enable: clique em *Enable* para ativar a função NTDP para a porta selecionada.

Disable: clique em *Disable* para desativar a função NTDP para a porta selecionada.

Obs.: *a função NTDP é eficaz somente quando a função está habilitada para a porta selecionada.*

13.3. Cluster

Um commander switch (Switch Principal) é capaz de reconhecer e adicionar os switches que estão diretamente conectados às redes.

A função de Cluster pode ser implementada na página *Cluster Summary* e *Cluster Config*.

Cluster summary

Nesta página você pode visualizar o status do Cluster corrente.

Escolha o menu *Cluster* → *Cluster* → *Cluster Summary* para carregar as seguintes páginas:

» Para o switch configurado como *Candidate*, a página apresenta o seguinte.

Status do switch Candidate

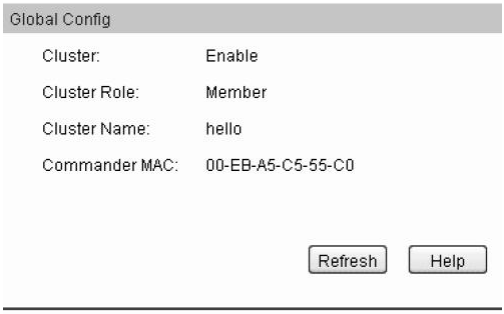
As seguintes opções são exibidas na tela:

» **Global config**

Cluster: exibe o status do Cluster Habilitado ou Desabilitado.

Cluster role: exibe a função do switch no Cluster.

» Para o switch configurado como *Member*, a seguinte página será exibida:



Status do switch Member

As seguintes opções são exibidas na tela:

» **Global config**
Cluster: exibe o status do Cluster (Ativado ou Desativado).
Cluster role: exibe a função do switch no Cluster.
Cluster name: exibe o nome do Cluster do qual o switch pertence.
Commander MAC: exibe o endereço MAC do Commander Switch (Switch Principal).

» Para o switch configurado como *Individual*, a seguinte página será exibida:

Status do switch Individual

As seguintes opções são exibidas na tela:

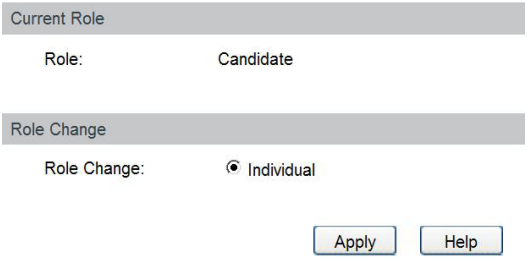
» **Global config**
Cluster: exibe o status do Cluster Habilitado ou Desabilitado.
Cluster role: exibe a função do switch no Cluster.

Cluster config

Nesta página você pode configurar a função do switch no Cluster

Escolha o menu *Cluster* → *Cluster* → *Cluster Config* para carregar a seguinte página:

» Para o switch configurado como *Candidate*, a página será a seguinte:



Configuração de Cluster para switch Candidate

As seguintes opções são exibidas na tela:

» **Current role**
Role: exibe a função atual do switch no Cluster.

» **Role change**

Individual: ao clicar em *Apply*, o switch mudará sua função para *Individual*.

» Para o switch configurado como *Individual*, a página exibe o seguinte:

Configuração de Cluster para switch Individual

As seguintes opções são exibidas na tela:

» **Current role**
Role: exibe a função atual do switch no Cluster.

» **Role change**
Candidate: ao clicar em *Apply*, o switch mudará sua função para *Candidate*.

13.4. Exemplo de aplicação da função Cluster

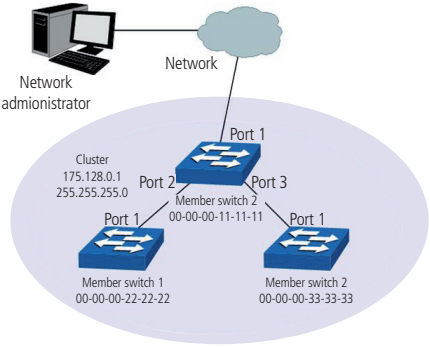
» **Requisitos de rede**

Três switches formam um Cluster. Um será o Commander Switch (Switch Principal) e dois serão membros. O administrador gerencia todos os switches do Cluster através do Commander Switch (Switch Principal).

» Na porta 1 do Commander Switch (Switch Principal) conecta-se a rede externa, na porta 2 conecta-se ao switch membro 1 e na porta 3 o switch membro 2.

» IP Pool: 175.128.0.1, Máscara: 255.255.255.0

» **Diagrama da rede**



Aplicação da função Cluster

» **Procedimento de configuração**

» Configuração do membro switch:

Step	Operation	Description
1	Habilite (Enable) a função NDP no switch para a porta1.	Na página Cluster⟶NDP⟶NDP Config habilite a função NDP.
2	Habilite a função NTDP no switch para a porta 1.	Na página Cluster⟶NTDP⟶NTDP Config Habilite a função NTDP.

» Configuração do Commander Switch (Switch Principal):

Step	Operation	Description
1	Habilite a função NDP no switch para as portas 1,2 e 3.	Na página Cluster⟶NDP⟶NDP Config Habilite a função NDP.
2	Habilite a função NTDP no switch para as portas 1,2 e 3.	Na página Cluster⟶NTDP⟶NTDP Config habilite a função NTDP.
3	Crie um Cluster e configure os parâmetros relacionados.	Na página Cluster⟶Cluster⟶Cluster Config configure Role como Commander Switch (Switch Principal) e insira as informações relacionadas. IP pool: 175.128.0.1 Mask: 255.255.255.0
4	Configuração do switch membro.	Na página Cluster⟶Cluster⟶Member Config, selecione o switch membro e clique em *Manage* para logar em sua web de gerenciamento.

14. Maintenance

No menu Maintenance é possível utilizar ferramentas para o diagnóstico da rede, fornecendo métodos para localização e solução de problemas.

1. System Monitor: monitora o status de utilização da memória e da CPU do switch.
2. Log: verifica os parâmetros de configuração do switch para descoberta de eventuais erros.
3. Cable Test: testa o status da conexão do cabo para localizar e diagnosticar problemas da rede.
4. Loopback: testa se as portas do switch e seu dispositivo conectado estão disponíveis.
5. Network Diagnose: testa se o dispositivo de destino é alcançável e detecta os saltos a partir do switch até o dispositivo de destino.

14.1. System monitor

A função System Monitor exibe o status de utilização da memória e da CPU do switch através de gráfico de utilização. A taxa de utilização da CPU e a taxa de utilização da memória devem apresentar-se de forma estável em torno de um valor específico. Se a taxa de utilização da CPU ou a taxa de utilização da memória aumentar muito, por favor, verifique se a rede está sendo atacada.

A função System Monitor é configurada em *CPU Monitor e Memory Monitor*

CPU monitor

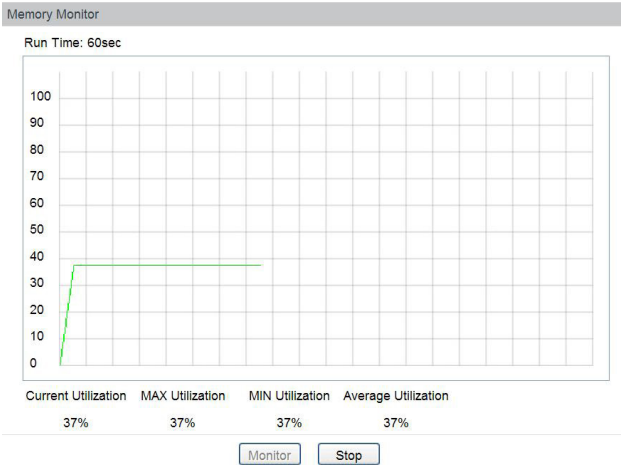
Escolha o menu *Maintenance* ⟶ *System Monitor* ⟶ *CPU Monitor* para carregar a seguinte página.

Monitoramento da CPU

Clique no botão *Monitor* para habilitar a função, o switch irá monitorar e exibir a taxa de utilização da CPU a cada quatro segundos.

Memory monitor

Escolha o menu *Maintenance* → *System Monitor* → *Memory Monitor* para carregar a seguinte página:



Monitoramento da memória

Clique no botão *Monitor* para habilitar a função, o switch irá monitorar e exibir a taxa de utilização da memória a cada quatro segundos.

14.2. Log

O sistema de Log do switch pode registrar, classificar e gerenciar as informações do sistema de forma eficaz, fornecendo um poderoso suporte para administração de redes, monitorando a operação da rede e diagnosticando avarias.

Os logs do switch são classificados nos seguintes níveis.

Gravidade	Nível	Descrição
emergencies	0	O sistema está inutilizável
alerts	1	Devem ser tomadas medidas imediatamente
critical	2	Condições críticas
errors	3	Condições de erro
warnings	4	Condições de alerta
notifications	5	Condições normais, mas significativas.
informational	6	Informações de mensagens
debugging	7	Nível de depuração de mensagens

A função Log é configurada em *Log Table, Local Log, Remote Log e Backup Log*.

Log table

O switch suporta dois meios para realização de Log, *Log Buffer* e *Log File*. As informações armazenadas em Buffer serão perdidas se o switch for reinicializado ou desligado, enquanto as informações no Log File serão mantidas.

Escolha o menu *Maintenance* → *Log* → *Log Table* para carregar a seguinte página:

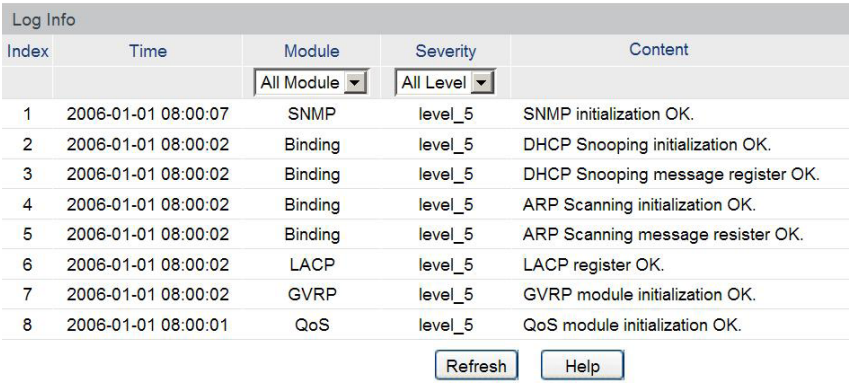

Log Info
Index
Time
Module
Severity
Content
All Module
All Level
1 2006-01-01 08:00:07 SNMP level_5 SNMP initialization OK.
2 2006-01-01 08:00:02 Binding level_5 DHCP Snooping initialization OK.
3 2006-01-01 08:00:02 Binding level_5 DHCP Snooping message register OK.
4 2006-01-01 08:00:02 Binding level_5 ARP Scanning initialization OK.
5 2006-01-01 08:00:02 Binding level_5 ARP Scanning message resister OK.
6 2006-01-01 08:00:02 LACP level_5 LACP register OK.
7 2006-01-01 08:00:02 GVRP level_5 GVRP module initialization OK.
8 2006-01-01 08:00:01 QoS level_5 QoS module initialization OK.
Refresh
Help
Note:
1.There are 8 severity levels marked with value 0-7. The smaller value has the higher priority.
2.This page displays logs in the log buffer, and at most 512 logs are displayed.

Tabela de Logs

As seguintes informações são exibidas na tela:

» **Log info**

Index: exibe o índice da informação de Log.

Time: exibe o momento em que o evento de Log ocorreu. O registro pode obter a hora correta após configurado a função System Time: *System → System Info → System Time.*

Module: exibe o módulo que as informações de Log pertencem.

Severity: exibe o nível da criticidade das informações.

Content: exibe o conteúdo das informações de Log.

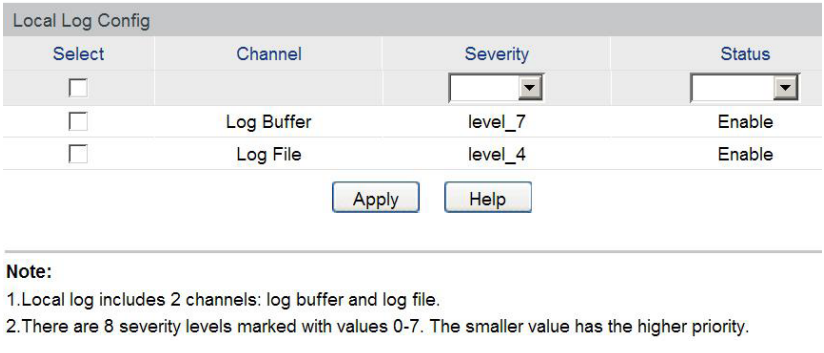
Obs.: » *Os registros de Logs são classificados em oito níveis de criticidade. Quanto maior a criticidade da informação, menor é o número Severity.*

» *Esta página exibe os Logs no Buffer de Log. São exibidos no máximo 512 registros.*

Local Log

Local Log é a informação de log salva no próprio switch. Por padrão, todos os logs de sistemas são salvos no Log Buffer e os logs com criticidade de nível 0 até o nível 4 são salvos no Log File. Nesta página você pode definir o canal de saída para Logs.

Escolha o menu *Maintenance → Log → Local Log* para carregar a seguinte página:



Local Log

As seguintes informações são apresentadas na tela:

» **Local Log config**

Select: selecione o canal correspondente para a configuração do Local Log.

Log buffer: indica que os Logs serão salvos na memória RAM. As informações no Buffer de Logs serão exibidas na página Log Table. Estas informações serão perdidas quando reiniciar o switch.

Log file: indica que os Logs serão salvos na memória Flash. As informações contidas no arquivo de Log não serão perdidas após o switch reiniciar e podem ser exportadas na página de backup de Log.

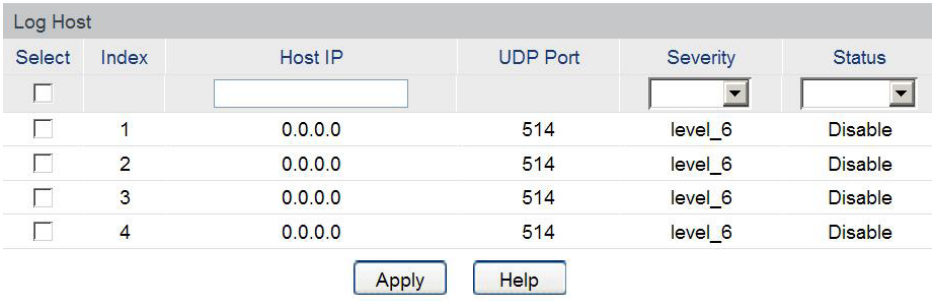
Severity: selecione o nível de criticidade da saída de informação de Log para cada canal. Apenas o Log com o nível de criticidade igual ou menor será armazenado.

Status: selecione *Enable/Disable* para habilitar ou desabilitar a função de Log Local no canal correspondente.

Remote Log

A função Remote Log permite que o switch envie os Logs do sistema para um servidor de Log. O servidor de Log serve para centralizar os Logs do sistema de vários dispositivos da rede.

Escolha o menu *Maintenance* → *Log* → *Remote Log* para carregar a seguinte página:



Log remoto

As seguintes informações são exibidas na tela:

» **Log Host**

Select: selecione o índice desejado para a configuração do servidor de Log remoto.

Index: exibe o índice do servidor de Log. É possível configurar até 4 servidores de Log remoto.

Host IP: digite o endereço IP do servidor de Log.

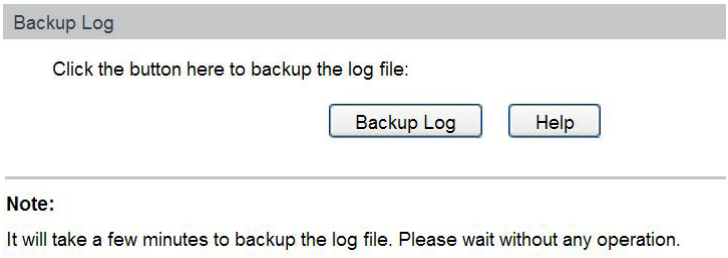
UDP Port: exibe a porta UDP usada para enviar/receber informações de Log. Por padrão, a porta utilizada é *514*.

Severity: selecione o nível de criticidade da informação de log enviada para o servidor de Log. Apenas os logs com o nível de criticidade igual ou menor ao selecionado serão enviados.

Backup Log

A função de Backup Log permite que o sistema registre as informações de Log do switch em arquivos, para ser feito uma análise posteriormente. Quando um erro crítico acontecer e o sistema entrar em colapso, você pode exportar os Logs após o switch ser reiniciado.

Escolha o menu *Maintenance* → *Log* → *Backup Log* para carregar a seguinte página.


Backup Log
Click the button here to backup the log file:
Backup Log
Help
Note:
It will take a few minutes to backup the log file. Please wait without any operation.

Backup de Log

As seguintes informações são apresentadas na tela:

» **Backup Log**

Backup Log: clique no botão *Backup Log* para salvar um arquivo com as informações de Log no seu computador.

Obs.: *levará alguns minutos para fazer o backup do arquivo de Log. Por favor, aguarde sem executar qualquer operação.*

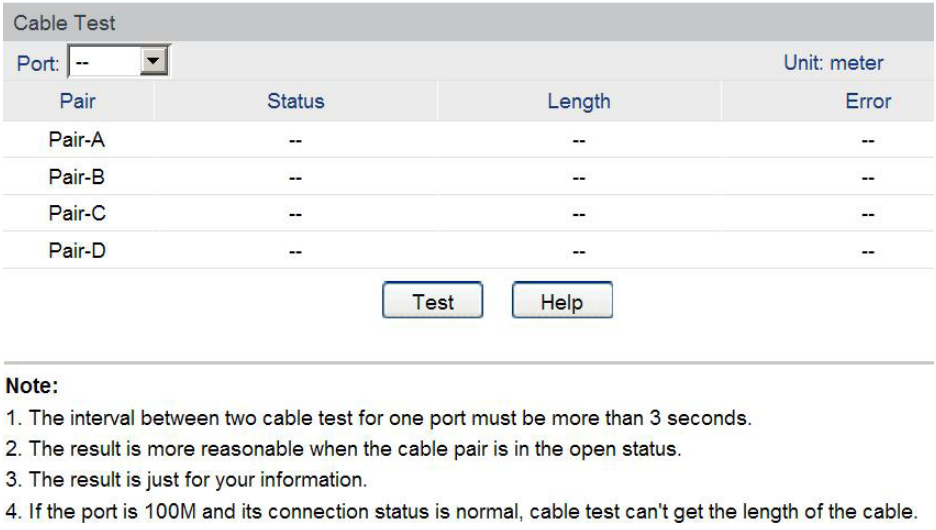
14.3. Device diagnose

Este switch oferece teste de cabo e de loopback para teste de conectividade das portas.

Cable test

A função Cable Test serve para testar o status da conexão do cabo conectado ao switch, o que facilita a localizar e diagnosticar os problemas da rede.

Escolha o menu *Maintenance* → *Device Diagnose* → *Cable Test* para carregar a seguinte página:


Cable Test
Port: --
Unit: meter
Pair
Status
Length
Error
Pair-A -- -- --
Pair-B -- -- --
Pair-C -- -- --
Pair-D -- -- --
Test
Help
Note:
1. The interval between two cable test for one port must be more than 3 seconds.
2. The result is more reasonable when the cable pair is in the open status.
3. The result is just for your information.
4. If the port is 100M and its connection status is normal, cable test can't get the length of the cable.

Teste de cabos

As seguintes informações são apresentadas na tela:

» **Cable test**

Port: selecione a porta para testar o cabo.

Pair: exibe o número do par.

Status: exibe o status da conexão do cabo conectado à porta. Os resultados do teste do cabo incluem: normal, fechado, aberto ou impedância.

Length: se o link está normal é exibido o comprimento do cabo.

Error: se o link está fechado, aberto ou impedância é exibido o erro de comprimento do cabo.

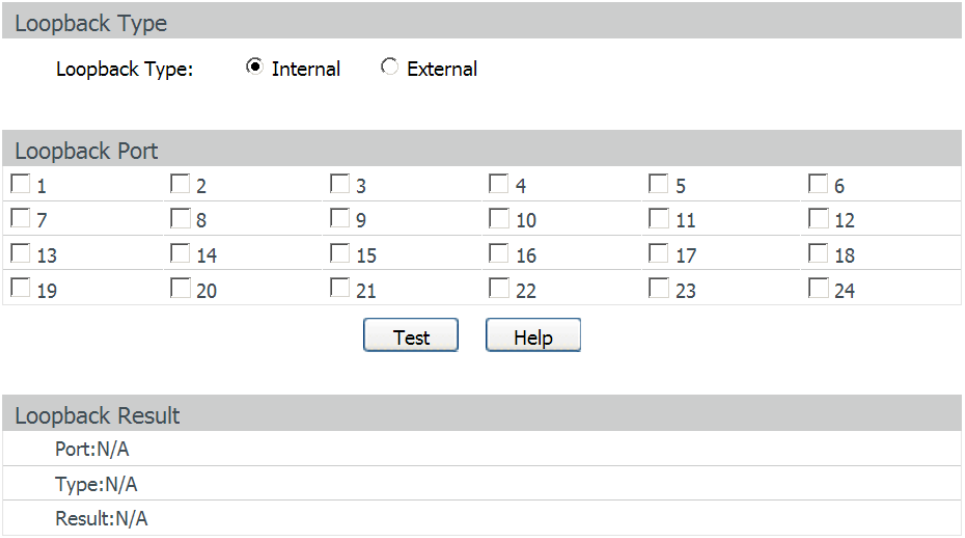
Obs.: » *O comprimento exibido é o comprimento dos pares interno do cabo, não do cabo físico em si.*

» *O resultado é apenas para sua referência.*

Loopback

A função Loopback é utilizada para testar a disponibilidade e analisar o status de uma porta física do switch. Esta função auxilia na solução de problemas na rede.

Escolha o menu *Maintenance* → *Device Diagnose* → *Loopback* para carregar a seguinte página.



Loopback

As seguintes opções são apresentadas na tela:

» **Loopback Type**

Internal: selecione a porta interna que deseja verificar se está ou não disponível.

External: selecione a porta externa que deseja verificar se o dispositivo conectado está ou não disponível.

» **Loopback Port**

Loopback Port: selecione a porta desejada para teste de loopback.

Test: clique no botão *Test* para iniciar o teste de loopback na porta.

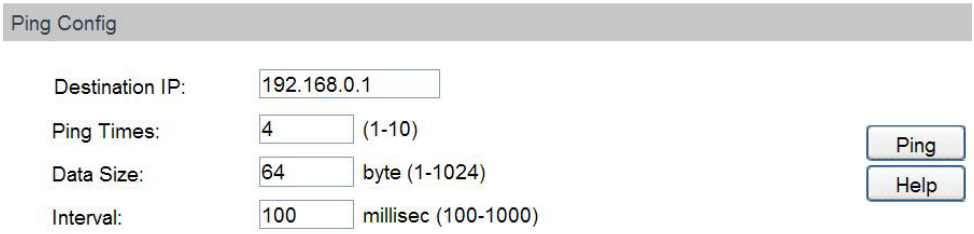
14.4. Network diagnose

Este switch oferece funções de teste de ping e Tracert para um melhor diagnostico da rede.

Ping

A função Ping testa a conectividade entre o switch e um dispositivo específico da rede, testando a conectividade entre o switch e os dispositivos da rede, facilitando a localização de falhas.

Escolha o menu *Maintenance* → *Network Diagnose* → *Ping* para carregar a seguinte página:



Ping

» **Ping config**

Destination IP: digite o endereço IP do dispositivo de destino para o teste de Ping.

Ping times: digite o tempo que a função ficará enviando dados.

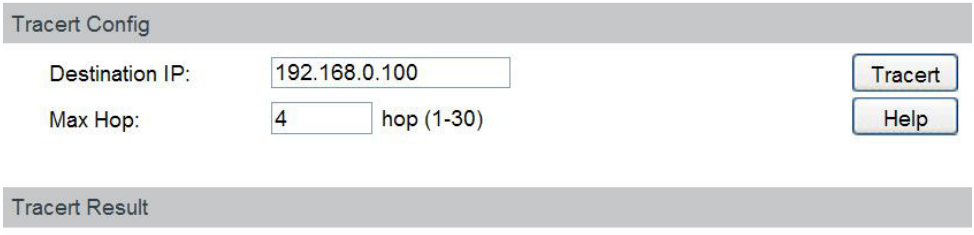
Data size: digite o tamanho dos pacotes enviados durante o Ping. O valor padrão é recomendado.

Interval: digite o intervalo de envio das requisições ICMP. O valor padrão é recomendado.

Tracert

A função Tracert é usada para descobrir o caminho feito pelos pacotes desde a sua origem até o seu destino, informando todos os gateways percorridos. Ele é usado para testes, medidas e gerenciamento da rede. O tracert pode ser utilizado para detectar falhas como, por exemplo, gateways que descartam pacotes ou rotas que excedem a capacidade de um datagrama IP.

Escolha o menu *Maintenance* → *Network Diagnose* → *Tracert* para carregar a seguinte página.



Tracert

As seguintes opções são apresentadas na tela:

» **Tracert config**

Destination IP: digite o endereço IP do dispositivo de destino.

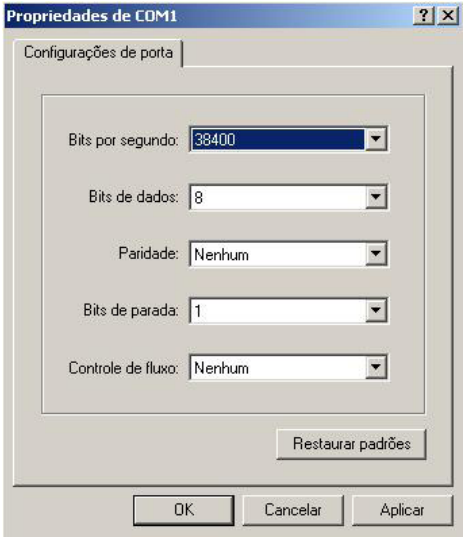
Max hop: digite o número máximo de saltos que poderá ser feito até chegar ao destino.

15. Restaurando para o padrão de fábrica

Para restaurar as configurações de fábrica do switch, deverá ser acessado o menu BootUtil via porta console, conforme instruções a seguir:

Acessando o menu BootUtil utilizando o Hyper Terminal:

Para exibir a interface de linha de comandos, conecte a extremidade (DB-9 fêmea) do cabo console na respectiva porta serial (COM) do computador e a outra extremidade (RJ45) na porta console (RJ45), localizada no painel frontal do switch. Abra o software Hyper Terminal com as seguintes configurações:



Configurando o Hyper Terminal

Taxa de dados: 38400 bits por segundo.

Formato dos dados: 8 bits de dados, sem paridade e 1 bit de parada.

Controle de fluxo: nenhum.

Para restaurar as configurações de fábrica do switch, é necessário entrar no menu BootUtil do switch, conforme os passos a seguir:

1. Com o PC conectado ao switch através da porta console, abra o software Hyper Terminal previamente configurado.
2. Desconecte e conecte o switch da rede elétrica. Quando lhe for pedido *"Press CTRL-B to enter the bootUtil"* no Hyper Terminal, por favor pressione as teclas *CTRL + B* para acessar o menu bootUtil, conforme imagem a seguir:

```
                    ************************************************
                    *        INTELBRAS  BOOTUTIL(v1.0.0)           *
                    ************************************************
                    Copyright (c) 2012 Intelbras S.A.
                    Create Date: Mar 30 2012 17:35:10

 help                       - print this list
 reboot                     - reboot the system
 ifconfig                   - config the interface
 ftp                        - config the remote host ip,the user name,user password
 and the image file name
 upgrade                    - upgrade the firmware
 start                      - start the system
 reset                      - reset the system to the factory config.

[INTELBRAS]:
```

Menu BootUtil

Obs.: *o processo entre ligar o switch e pressionar as teclas CRTL + B é extremamente rápido, recomendamos que as teclas CTRL + B sejam pressionadas no momento em que o switch está sendo ligado.*

Após ter acessado o menu BootUtil, realize os seguintes comandos:

» ***Reset*** (para restaurar o switch com as configurações de fábrica, conforme imagem a seguir).

****
* INTELBRAS BOOTUTIL(v1.0.0) *
****
Copyright (c) 2012 Intelbras S.A.
Create Date: Mar 30 2012 17:35:10
help - print this list
reboot - reboot the system
ifconfig - config the interface
ftp - config the remote host ip,the user name,user password
and the image file name
upgrade - upgrade the firmware
start - start the system
reset - reset the system to the factory config.
[INTELBRAS]: reset_

Menu BootUtil - restaurar

» ***Reiniciar*** (para reiniciar o switch com as configurações de fábrica, conforme imagem a seguir).

****
* INTELBRAS BOOTUTIL(v1.0.0) *
****
Copyright (c) 2012 Intelbras S.A.
Create Date: Mar 30 2012 17:35:10
help - print this list
reboot - reboot the system
ifconfig - config the interface
ftp - config the remote host ip,the user name,user password
and the image file name
upgrade - upgrade the firmware
start - start the system
reset - reset the system to the factory config.
[INTELBRAS]: reset
[INTELBRAS]: reboot_

Menu BootUtil - reiniciar

Termo de garantia

Para a sua comodidade, preencha os dados abaixo, pois, somente com a apresentação deste em conjunto com a nota fiscal de compra do produto, você poderá utilizar os benefícios que lhe são assegurados.

Nome do cliente:

Assinatura do cliente:

Nº da nota fiscal:

Data da compra:

Modelo: Nº de série:

Revendedor:

Fica expresso que esta garantia contratual é conferida mediante as seguintes condições:

1. Todas as partes, peças e componentes do produto são garantidos contra eventuais defeitos de fabricação que porventura venham a apresentar, pelo prazo de 3 (três) anos, sendo este prazo de 3 (três) meses de garantia legal mais 33 (trinta e três) meses de garantia contratual, contado a partir da data de entrega do produto ao Senhor Consumidor, conforme consta na nota fiscal de compra do produto, que é parte integrante deste Termo em todo território nacional. Esta garantia contratual implica na troca gratuita das partes, peças e componentes que apresentarem defeito de fabricação, além da mão-de-obra utilizada nesse reparo. Caso não seja constatado defeito de fabricação, e sim defeito(s) proveniente(s) de uso inadequado, o Senhor Consumidor arcará com estas despesas.
2. Constatado o defeito, o Senhor Consumidor deverá imediatamente comunicar-se com o Serviço Autorizado mais próximo que consta na relação oferecida pelo fabricante - somente estes estão autorizados a examinar e sanar o defeito durante o prazo de garantia aqui previsto. Se isto não for respeitado esta garantia perderá sua validade, pois o produto terá sido violado.
3. Na eventualidade do Senhor Consumidor solicitar o atendimento domiciliar, deverá encaminhar-se ao Serviço Autorizado mais próximo para consulta da taxa de visita técnica. Caso seja constatada a necessidade da retirada do produto, as despesas decorrentes, transporte, segurança de ida e volta do produto, ficam sob a responsabilidade do Senhor Consumidor.
4. A garantia perderá totalmente sua validade se ocorrer qualquer das hipóteses a seguir: a) se o defeito não for de fabricação, mas sim, ter sido causado pelo Senhor Consumidor ou terceiros estranhos ao fabricante; b) se os danos ao produto forem oriundos de acidentes, sinistros, agentes da natureza (raios, inundações, desabamentos, etc.), umidade, tensão na rede elétrica (sobretensão provocada por acidentes ou flutuações excessivas na rede), instalação/uso em desacordo com o Manual do Usuário ou decorrente do desgaste natural das partes, peças e componentes; c) se o produto tiver sofrido influência de natureza química, eletromagnética, elétrica ou animal (insetos, etc.); d) se o número de série do produto houver sido adulterado ou rasurado; e) se o aparelho houver sido violado.

Sendo estas condições deste Termo de Garantia complementar, a Intelbras S/A reserva-se o direito de alterar as características gerais, técnicas e estéticas de seus produtos sem aviso prévio.

O processo de fabricação deste produto não está coberto pelo sistema de gestão ambiental da Intelbras.

Todas as imagens deste manual são ilustrativas.

intelbras

eco amigável

uma das melhores
empresas para se trabalhar

fale com a gente

Suporte a clientes: (48) 2106 0006
Contato e chat: www.intelbras.com.br/suporte
Sugestões, reclamações e rede autorizada: 0800 7042767

Intelbras S/A – Indústria de Telecomunicação Eletrônica Brasileira
Rodovia BR 101, km 213 - Área Industrial - São José/SC - 88104-800
www.intelbras.com.br

01.12